

# **LAPORAN PRAKTIKUM**

## **VULNERABILITY AND SOCIAL ENGINEERING**



### **DISUSUN OLEH :**

Nama : Diki Candra  
Nim : 2022903430010  
Kelas : TRKJ 2B  
Jurusan : Teknologi Informasi dan Komputer  
Program Studi : Teknologi Rekayasa Komputer Jaringan  
Dosen Pengajar : Aswandi, S.Kom, M.Kom.

**JURUSAN TEKNOLOGI INFORMASI DAN KOMUNIKASI**  
**PRODI TEKNOLOGI REKAYASA KOMPUTER DAN**  
**JARINGAN**  
**POLITEKNIK NEGERI LHOKSEUMAWE**  
**TAHUN 2022/2023**

## LEMBARAN PENGESAHAN

Laporan Yang Berjudul : Vulnerability And Social Engineering  
Disusun Oleh : Diki Candra  
NIM : 2022903430010  
Tanggal Praktikum : 18 September 2023  
Tanggal Penyerahan : 25 September 2023  
Jurusan : Teknologi Informasi & Komputer  
Program Studi : Teknologi Rekayasa Komputer Jaringan  
Mata Kuliah : Ethical Hacking  
Tabel Penilaian :



Mengetahui,

Dosen Pembimbing,

Penyusun,

Aswandi, S.Kom, M.Kom  
NIP. 197209242010121001

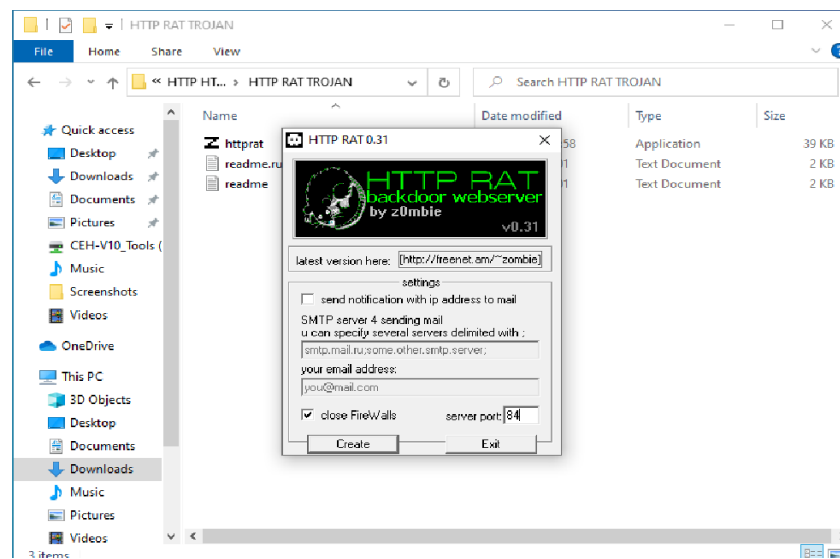
Diki Candra  
NIM. 2022903430010

## PERCOBAAN 1

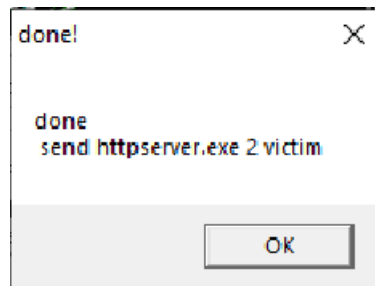
- Klik dua kali httpprat.exe, jendela utama HTTP RAT muncul seperti gambar di bawah ini



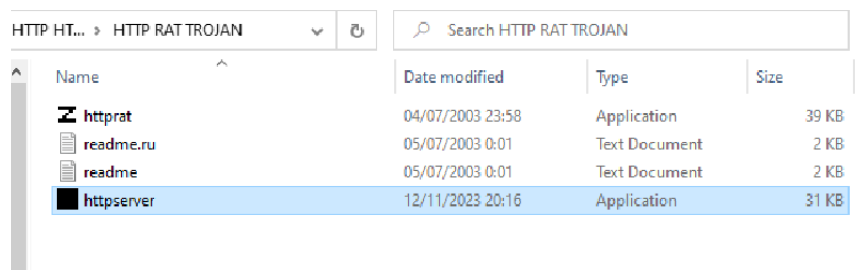
- Hapus centang kirim pemberitahuan dengan alamat IP ke email pilihan, masukkan port server ke 84 dan klik Buat.



- Setelah file httpserver.exe dibuat, pop-up akan ditampilkan, klik OK dan bagikan file dengan mesin virtual Windows 10.



- Sekarang masuk ke Windows 10 dan arahkan ke tempat Anda menyimpan file httpserver.exe. Klik dua kali untuk menjalankan Trojan.



- Kita akan dapat melihat proses Httpserver di task manager:

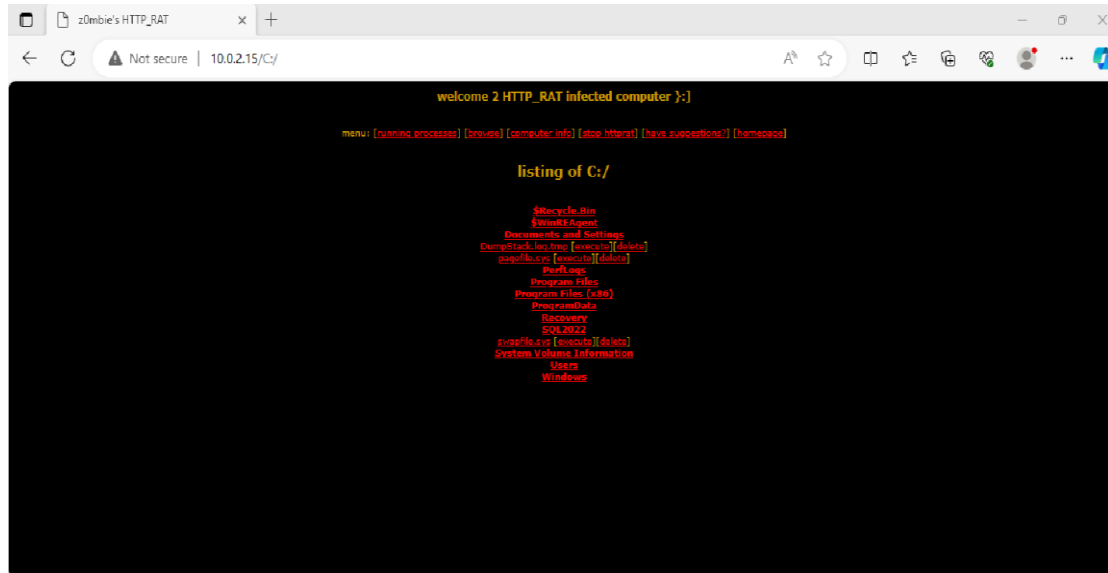
| Task Manager   |        |         |            |          |            |             |                  |
|--|--------|---------|------------|----------|------------|-------------|------------------|
| File Options View  |        |         |            |          |            |             |                  |
| Processes Performance App history Startup Users Details Services |        |         |            |          |            |             |                  |
| Name   | Status | 10% CPU | 52% Memory | 0% Disk  | 0% Network | Power usage | Power usage t... |
| > Antimalware Service Executable                                 |        | 0%      | 71,7 MB    | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| Application Frame Host   |        | 0%      | 3,0 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| COM Surrogate  |        | 0%      | 1,6 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| COM Surrogate  |        | 0%      | 2,0 MB     | 0,1 MB/s | 0 Mbps     | Very low    | Very low         |
| CTF Loader   |        | 0%      | 2,5 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| Google Crash Handler   |        | 0%      | 0,1 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| Google Crash Handler (32 bit)                                    |        | 0%      | 0,4 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| Host Process for Windows Tasks                                   |        | 0%      | 0,6 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| httpserver (32 bit)  |        | 0%      | 0,9 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| Microsoft OneDrive   |        | 0%      | 6,9 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| Microsoft OneDriveFile Co-Aut...                                 |        | 0%      | 1,2 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| > Microsoft Text Input Application                               |        | 0%      | 2,8 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| Microsoft Windows Search Filte...                                |        | 0%      | 1,0 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |
| > Microsoft Windows Search Inde...                               |        | 0%      | 9,0 MB     | 0 MB/s   | 0 Mbps     | Very low    | Very low         |

- Beralih kembali ke Windows Server 2012 dan luncurkan browser web.

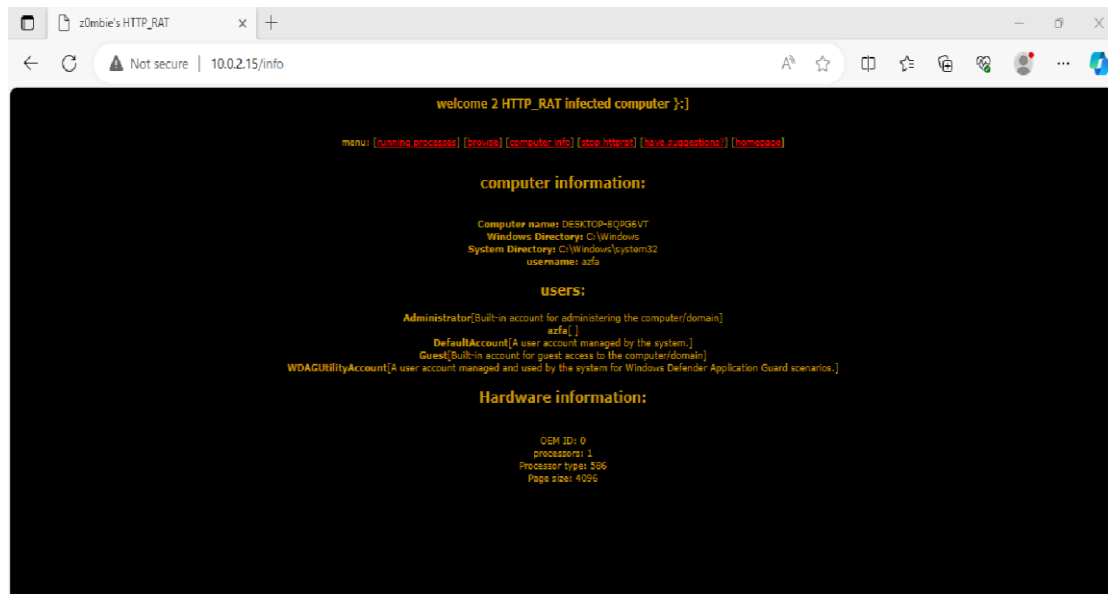
- 
- The screenshot shows a web browser window with the address bar displaying 'z0mbie's HTTP\_RAT' and the URL '10.0.2.15'. The browser's address bar also shows 'Not secure'. The main content area is a black terminal window with yellow text. The terminal displays a yellow prompt 'welcome 2 HTTP\_RAT infected computer >:', followed by a red menu list: 'menu: (running processes) (browser) (computer info) (steal httpcat) (have suggestions?) (homepage)'. Below the menu, the terminal displays a yellow prompt 'welcome >:'.

- [illegible]

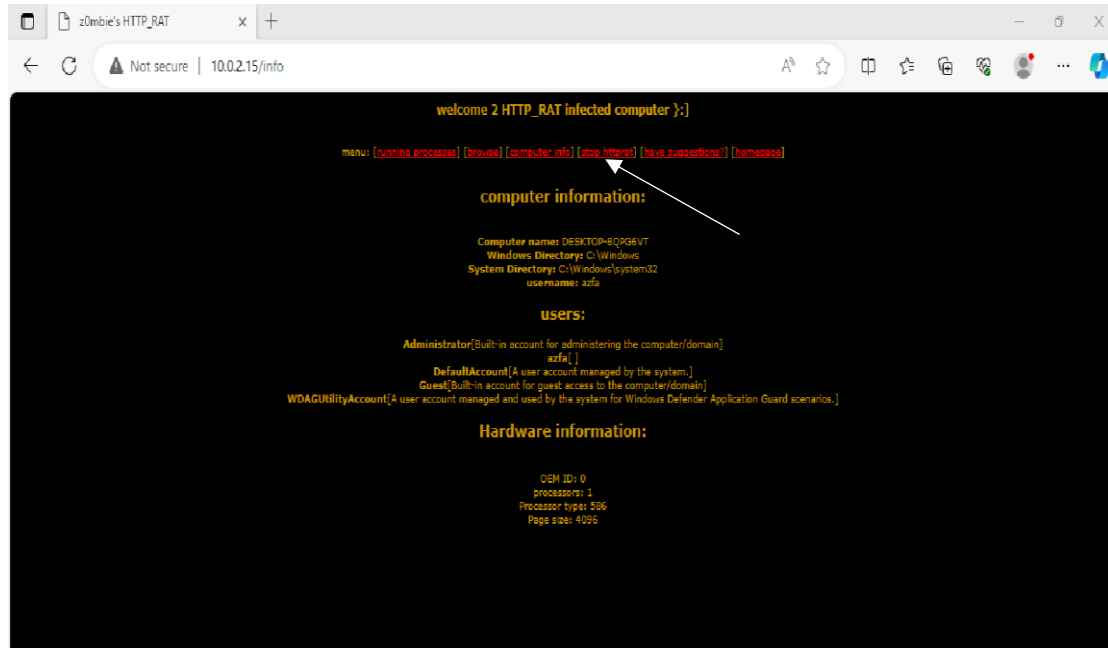
- Klik browse dan kemudian klik Drive C untuk menjelajahi konten di drive ini.



- Klik info komputer untuk melihat informasi komputer, pengguna, dan perangkat keras.



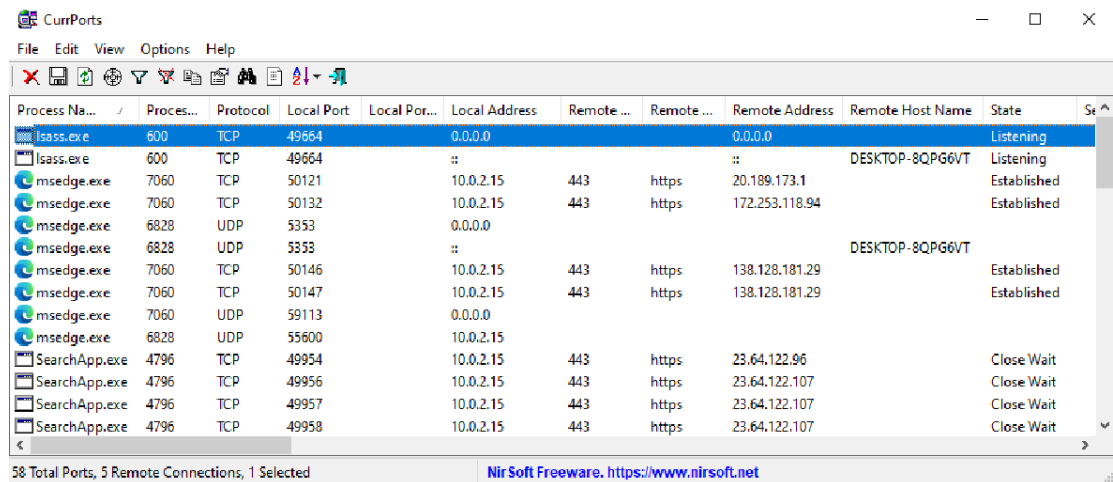
- Setelah selesai, Klik Stop Httpserver.exe di Windows 10.



## PERCOBAAN 2

### Download tool Currports

- Buka Tools nya seperti Berikut



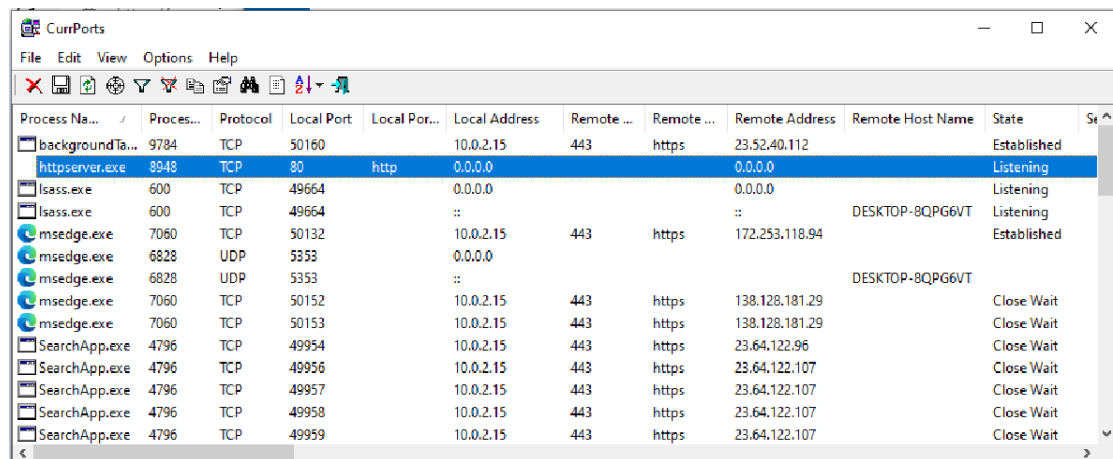
The screenshot shows the CurrPorts application window. The title bar is 'CurrPorts'. The menu bar includes 'File', 'Edit', 'View', 'Options', and 'Help'. The toolbar contains various icons for file operations and network analysis. The main table displays the following data:

| Process Name  | Process ID | Protocol | Local Port | Local Port... | Local Address | Remote ... | Remote ... | Remote Address | Remote Host Name | State       | Se ^ |
|---------------|------------|----------|------------|---------------|---------------|------------|------------|----------------|------------------|-------------|------|
| lsass.exe     | 600        | TCP      | 49664      |               | 0.0.0.0       |            |            | 0.0.0.0        |                  | Listening   |      |
| lsass.exe     | 600        | TCP      | 49664      |               | ::            |            |            | ::             | DESKTOP-8QPG6VT  | Listening   |      |
| msedge.exe    | 7060       | TCP      | 50121      |               | 10.0.2.15     | 443        | https      | 20.189.173.1   |                  | Established |      |
| msedge.exe    | 7060       | TCP      | 50132      |               | 10.0.2.15     | 443        | https      | 172.253.118.94 |                  | Established |      |
| msedge.exe    | 6828       | UDP      | 5353       |               | 0.0.0.0       |            |            |                |                  |             |      |
| msedge.exe    | 6828       | UDP      | 5353       |               | ::            |            |            |                | DESKTOP-8QPG6VT  |             |      |
| msedge.exe    | 7060       | TCP      | 50146      |               | 10.0.2.15     | 443        | https      | 138.128.181.29 |                  | Established |      |
| msedge.exe    | 7060       | TCP      | 50147      |               | 10.0.2.15     | 443        | https      | 138.128.181.29 |                  | Established |      |
| msedge.exe    | 7060       | UDP      | 59113      |               | 0.0.0.0       |            |            |                |                  |             |      |
| msedge.exe    | 6828       | UDP      | 55600      |               | 10.0.2.15     |            |            |                |                  |             |      |
| SearchApp.exe | 4796       | TCP      | 49954      |               | 10.0.2.15     | 443        | https      | 23.64.122.96   |                  | Close Wait  |      |
| SearchApp.exe | 4796       | TCP      | 49956      |               | 10.0.2.15     | 443        | https      | 23.64.122.107  |                  | Close Wait  |      |
| SearchApp.exe | 4796       | TCP      | 49957      |               | 10.0.2.15     | 443        | https      | 23.64.122.107  |                  | Close Wait  |      |
| SearchApp.exe | 4796       | TCP      | 49958      |               | 10.0.2.15     | 443        | https      | 23.64.122.107  |                  | Close Wait  |      |

58 Total Ports, 5 Remote Connections, 1 Selected

NirSoft Freeware. <https://www.nirsoft.net>

- Jalankan HTTPserver.exe di Trojan

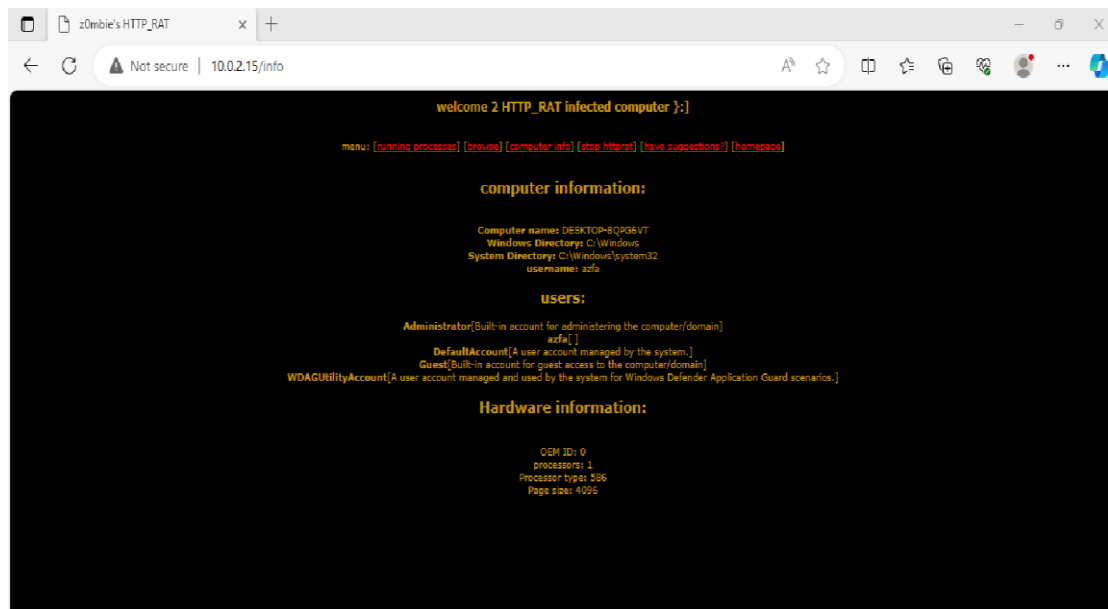
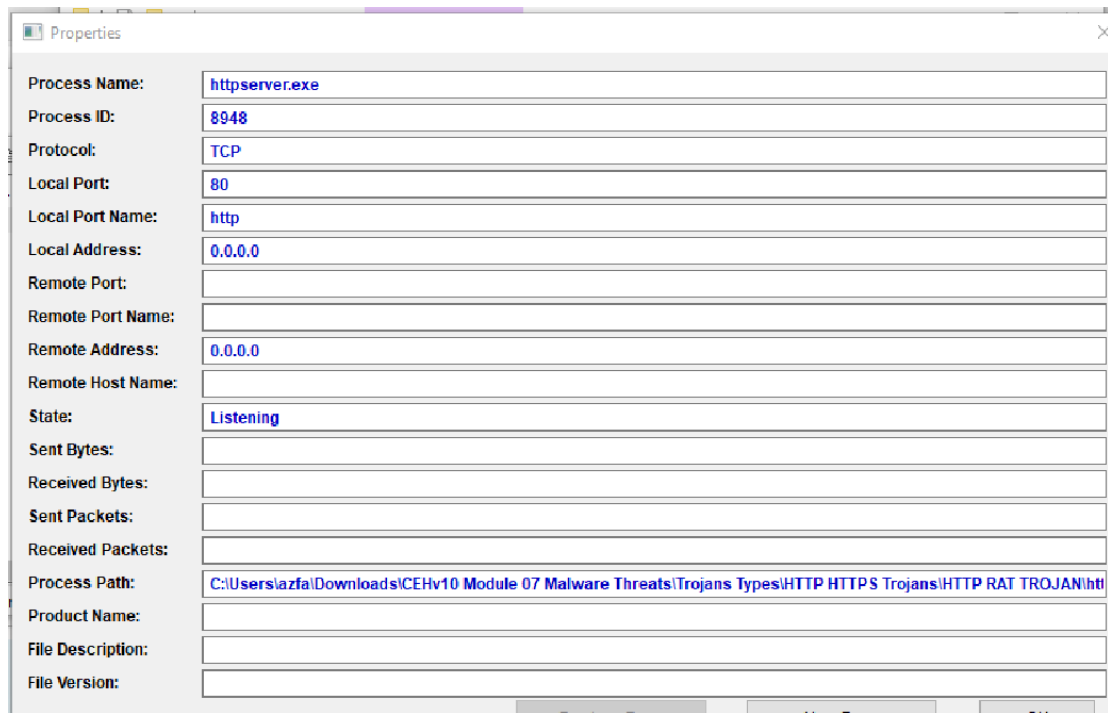


The screenshot shows the CurrPorts application window after running httpserver.exe. The table now includes the following data:

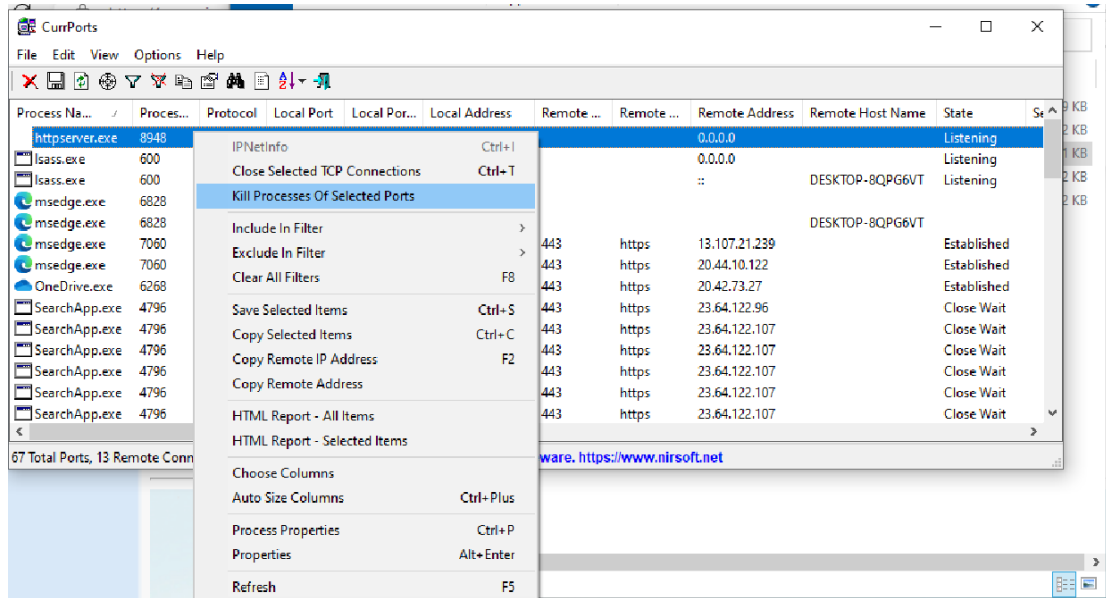
| Process Name    | Process ID | Protocol | Local Port | Local Port... | Local Address | Remote ... | Remote ... | Remote Address | Remote Host Name | State       | Se ^ |
|-----------------|------------|----------|------------|---------------|---------------|------------|------------|----------------|------------------|-------------|------|
| backgroundTa... | 9784       | TCP      | 50160      |               | 10.0.2.15     | 443        | https      | 23.52.40.112   |                  | Established |      |
| httpserver.exe  | 8948       | TCP      | 80         | http          | 0.0.0.0       |            |            | 0.0.0.0        |                  | Listening   |      |
| lsass.exe       | 600        | TCP      | 49664      |               | 0.0.0.0       |            |            | 0.0.0.0        |                  | Listening   |      |
| lsass.exe       | 600        | TCP      | 49664      |               | ::            |            |            | ::             | DESKTOP-8QPG6VT  | Listening   |      |
| msedge.exe      | 7060       | TCP      | 50132      |               | 10.0.2.15     | 443        | https      | 172.253.118.94 |                  | Established |      |
| msedge.exe      | 6828       | UDP      | 5353       |               | 0.0.0.0       |            |            |                |                  |             |      |
| msedge.exe      | 6828       | UDP      | 5353       |               | ::            |            |            |                | DESKTOP-8QPG6VT  |             |      |
| msedge.exe      | 7060       | TCP      | 50152      |               | 10.0.2.15     | 443        | https      | 138.128.181.29 |                  | Close Wait  |      |
| msedge.exe      | 7060       | TCP      | 50153      |               | 10.0.2.15     | 443        | https      | 138.128.181.29 |                  | Close Wait  |      |
| SearchApp.exe   | 4796       | TCP      | 49954      |               | 10.0.2.15     | 443        | https      | 23.64.122.96   |                  | Close Wait  |      |
| SearchApp.exe   | 4796       | TCP      | 49956      |               | 10.0.2.15     | 443        | https      | 23.64.122.107  |                  | Close Wait  |      |
| SearchApp.exe   | 4796       | TCP      | 49957      |               | 10.0.2.15     | 443        | https      | 23.64.122.107  |                  | Close Wait  |      |
| SearchApp.exe   | 4796       | TCP      | 49958      |               | 10.0.2.15     | 443        | https      | 23.64.122.107  |                  | Close Wait  |      |
| SearchApp.exe   | 4796       | TCP      | 49959      |               | 10.0.2.15     | 443        | https      | 23.64.122.107  |                  | Close Wait  |      |



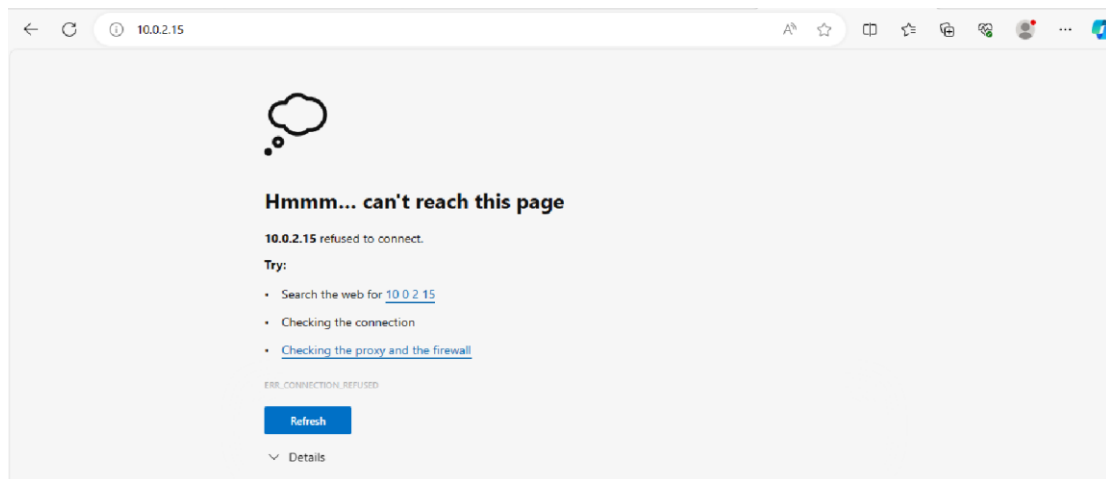
- Melihat info / Mengamati nama Proses , Protkol ,port lokal, dan Jarak jauh serta Informasi alamat ip



- Kembali ke windows untuk Mematikan Koneksi



- Setelah Koneksi dimatikan , Search lagi ip yang dibrowser



## **Kesimpulan:**

### **1. HTTP RAT (Remote Access Trojan):**

- Penggunaan HTTP RAT dimulai dengan menjalankan **httprat.exe** pada Windows Server 2012.
- Konfigurasi trojan dilakukan dengan menghapus opsi pengiriman pemberitahuan melalui email, mengatur port server ke 84, dan membuat file **httpserver.exe**.
- Setelah file **httpserver.exe** dibuat, dijalankan pada Windows 10, dan trojan berhasil terbentuk.
- Pada Windows Server 2012, akses ke mesin Windows 10 dilakukan melalui browser dengan memasukkan alamat IP Windows 10.
- Tools trojan menyediakan fungsionalitas seperti melihat proses yang berjalan, membunuh proses, menjelajahi isi drive C, dan melihat informasi sistem.

### **2. CurrPorts Tool:**

- Pada percobaan kedua, digunakan tool CurrPorts untuk memantau koneksi jaringan pada sistem.
- HTTPserver.exe dijalankan untuk membuat koneksi, dan CurrPorts digunakan untuk melihat informasi tentang proses, protokol, port lokal, alamat IP lokal, dan alamat IP jarak jauh.
- Setelah itu, koneksi dari HTTPserver.exe dimatikan, dan CurrPorts digunakan lagi untuk memverifikasi pemutusan koneksi.

**Keseluruhan:** Percobaan tersebut mengilustrasikan bagaimana sebuah HTTP RAT dapat digunakan untuk mendapatkan akses ke sistem target, memantau proses, dan melakukan operasi lainnya. Pemahaman tentang alat-alat seperti CurrPorts juga diperlihatkan untuk memantau dan mengontrol koneksi jaringan.

