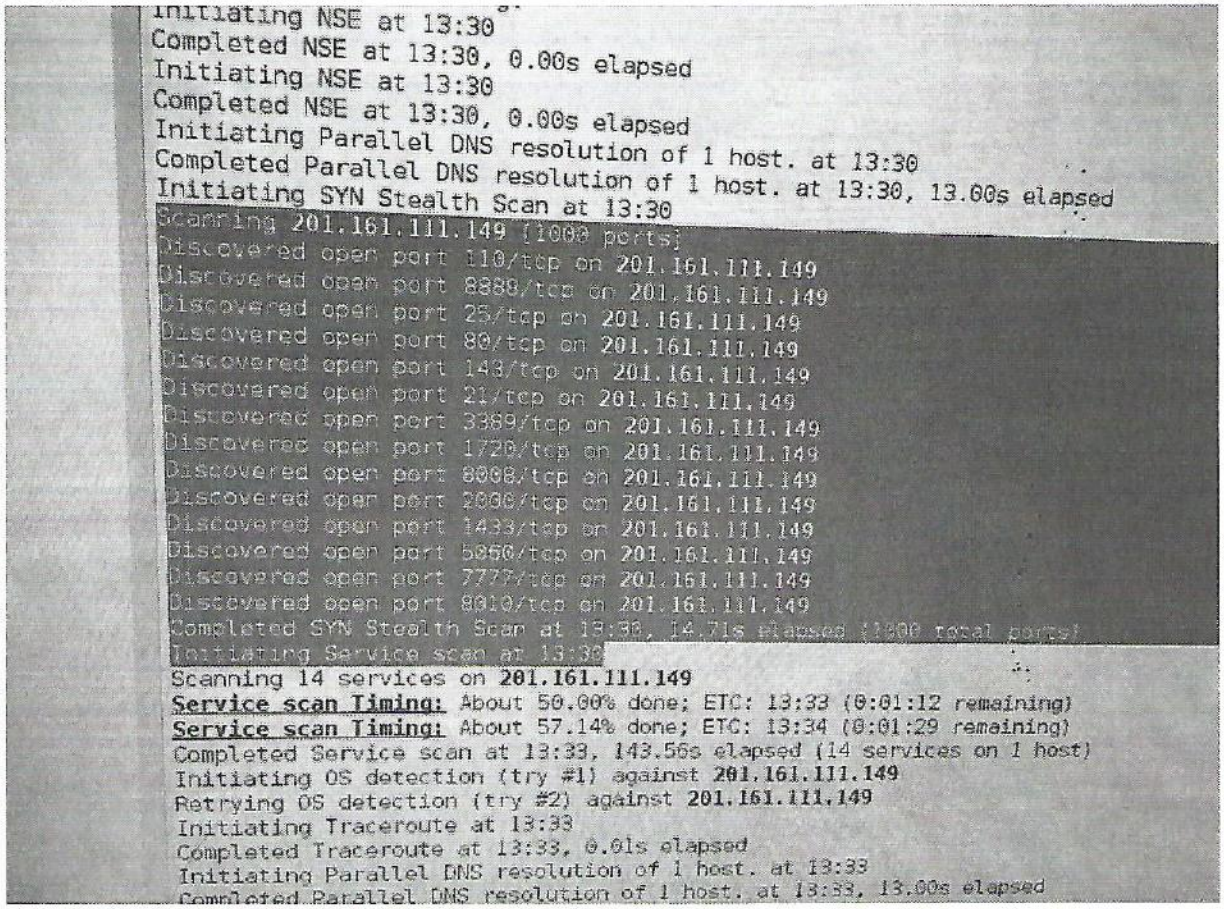
Reporte de Escaneo de Puertos y denegación de servicios DDOS del sitio del PREP Tlaxcala

Instituto Tlaxcalteca Electoral 5 de Junio 2016

Escaneo de Puertos

El día 3 de Junio se realizó un escaneo de puertos al sitio que contiene el sistema PREP del Instituto Tlaxcalteca de elecciones, con herramientas de escaneo llamada Zenmap, a la dirección 201.161.111.149, después de terminar el escaneo la aplicación arrojo información indicando varios puertos abiertos los cuales comprometen la seguridad del servidor.

Juan Carlos Olivares



```
Initiating NSE at 13:30
Completed NSE at 13:30, 0.00s elapsed
Initiating NSE at 13:30
Completed NSE at 13:30, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 13:30
Completed Parallel DNS resolution of 1 host. at 13:30, 13.00s elapsed
Initiating SYN Stealth Scan at 13:30
Scanning 201.161.111.149 [1000 ports]
Discovered open port 110/tcp on 201.161.111.149
Discovered open port 8888/tcp on 201.161.111.149
Discovered open port 25/tcp on 201.161.111.149
Discovered open port 80/tcp on 201.161.111.149
Discovered open port 143/tcp on 201.161.111.149
Discovered open port 21/tcp on 201.161.111.149
Discovered open port 3389/tcp on 201.161.111.149
Discovered open port 1720/tcp on 201.161.111.149
Discovered open port 8008/tcp on 201.161.111.149
Discovered open port 2000/tcp on 201.161.111.149
Discovered open port 1433/tcp on 201.161.111.149
Discovered open port 5060/tcp on 201.161.111.149
Discovered open port 7777/tcp on 201.161.111.149
Discovered open port 8010/tcp on 201.161.111.149
Completed SYN Stealth Scan at 13:30, 14.71s elapsed (1000 total ports)
Initiating Service scan at 13:30
Scanning 14 services on 201.161.111.149
Service scan Timing: About 50.00% done; ETC: 13:33 (0:01:12 remaining)
Service scan Timing: About 57.14% done; ETC: 13:34 (0:01:29 remaining)
Completed Service scan at 13:33, 143.56s elapsed (14 services on 1 host)
Initiating OS detection (try #1) against 201.161.111.149
Retrying OS detection (try #2) against 201.161.111.149
Initiating Traceroute at 13:33
Completed Traceroute at 13:33, 0.01s elapsed
Initiating Parallel DNS resolution of 1 host. at 13:33
Completed Parallel DNS resolution of 1 host. at 13:33, 13.00s elapsed
```

IMG1.- Resultado de escaneo de Puertos de Servidor PREP Tlaxcala

Derivado de este análisis se informó al personal del centro de cómputo del Instituto Tlaxcalteca de elecciones para que cerraran todos aquellos puertos que no son requeridos para el funcionamiento del PREP, una vez notificados del cierre de puertos se realizó un nuevo escaneo el cual arrojo los siguientes resultados.

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-12-02 15:33 PST
NSE: Loaded 122 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Initiating Ping Scan at 15:33
Scanning 201.161.111.149 [4 ports]
Completed Ping Scan at 15:33, 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:33
```

Juan Carl(c) Olivares

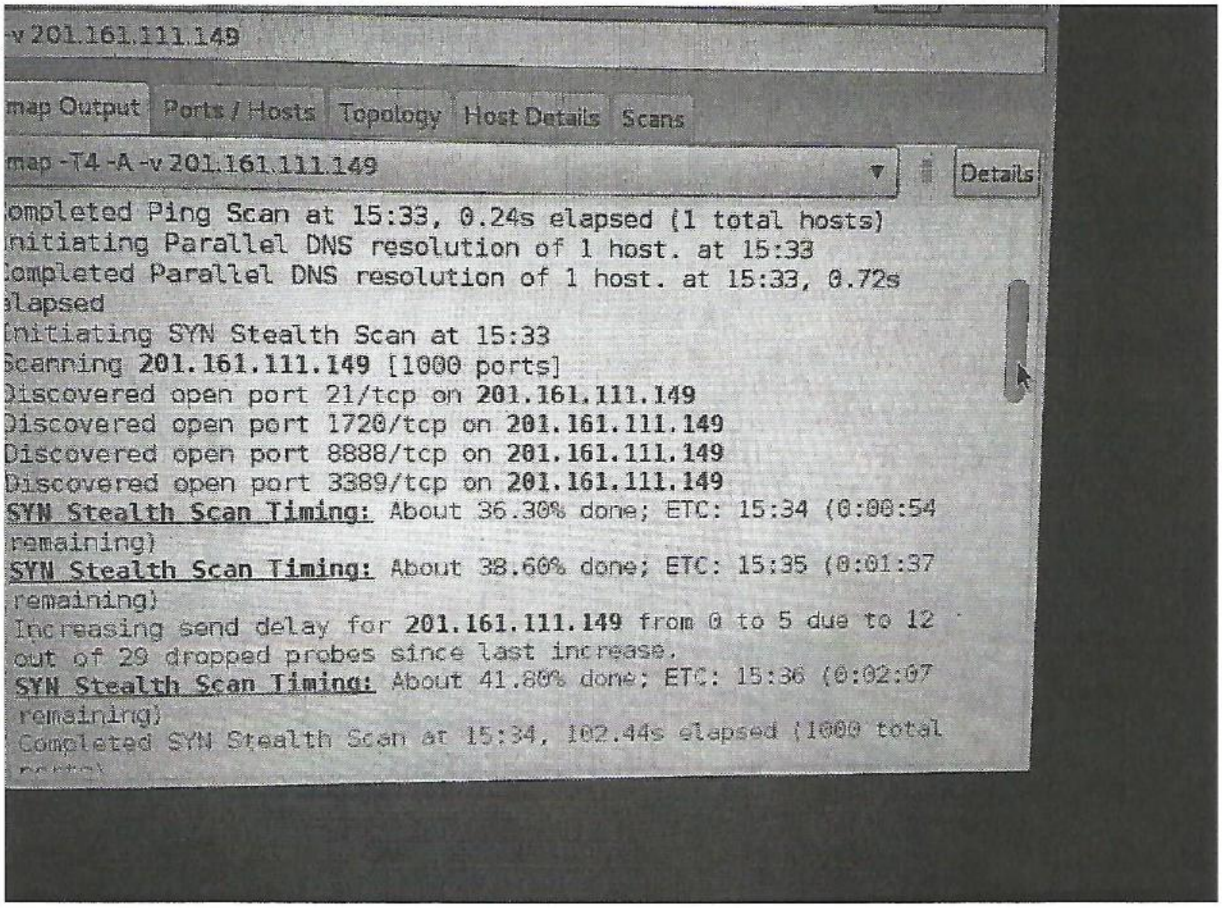
```
Completed Parallel DNS resolution of 1 host. at 15:33, 0.72s elapsed
Initiating SYN Stealth Scan at 15:33
Scanning 201.161.111.149 [1000 ports]
Discovered open port 21/tcp on 201.161.111.149
Discovered open port 1720/tcp on 201.161.111.149
Discovered open port 8888/tcp on 201.161.111.149
Discovered open port 3389/tcp on 201.161.111.149
SYN  Stealth  Scan  Timing:  About  36.30%  done;  ETC:  15:34  (0:00:54
remaining)
SYN  Stealth  Scan  Timing:  About  38.60%  done;  ETC:  15:35  (0:01:37
remaining)
Increasing send delay for 201.161.111.149 from 0 to 5 due to 12 out of
29 dropped probes since last increase.
SYN  Stealth  Scan  Timing:  About  41.80%  done;  ETC:  15:36  (0:02:07
remaining)
Completed  SYN  Stealth  Scan  at  15:34,  102.44s  elapsed  (1000  total
ports)
Initiating Service scan at 15:34
Scanning 4 services on 201.161.111.149
Completed Service scan at 15:35, 43.88s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 201.161.111.149
Initiating Traceroute at 15:35
Completed Traceroute at 15:35, 0.03s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 15:35
Completed Parallel DNS resolution of 2 hosts. at 15:35, 0.32s elapsed
NSE: Script scanning 201.161.111.149.
Initiating NSE at 15:35
Completed NSE at 15:36, 43.99s elapsed
Initiating NSE at 15:36
Completed NSE at 15:36, 0.00s elapsed
Nmap scan report for 201.161.111.149
Host is up (0.011s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
|_ftp-anon: ERROR: Script execution failed (use -d to debug)
1720/tcp open  h323q931?
3389/tcp open  tcpwrapped
8888/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec Linux, Linux 2.4.X|3.X, Microsoft Windows 7|2012|XP
OS  CPE:  cpe:/o:actiontec:linux_kernel  cpe:/o:linux:linux_kernel:2.4
cpe:/o:linux:linux_kernel:3                     cpe:/o:microsoft:windows_7
cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows_xp::sp3
OS  details:  Actiontec  MI424WR-GEN3I  WAP,  DD-WRT  v24-sp2  (Linux
2.4.37),  Linux  3.2,  Microsoft  Windows  7  or  Windows  Server  2012,
Microsoft Windows XP SP3
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
```

Juan Carlos Olivares

```
IP ID Sequence Generation: Incremental

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.10 ms 192.168.184.2
2   0.10 ms 201.161.111.149

NSE: Script Post-scanning.
Initiating NSE at 15:36
Completed NSE at 15:36, 0.00s elapsed
Initiating NSE at 15:36
Completed NSE at 15:36, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 196.82 seconds
           Raw packets sent: 3094 (138.548KB) | Rcvd: 330 (13.324KB)
```



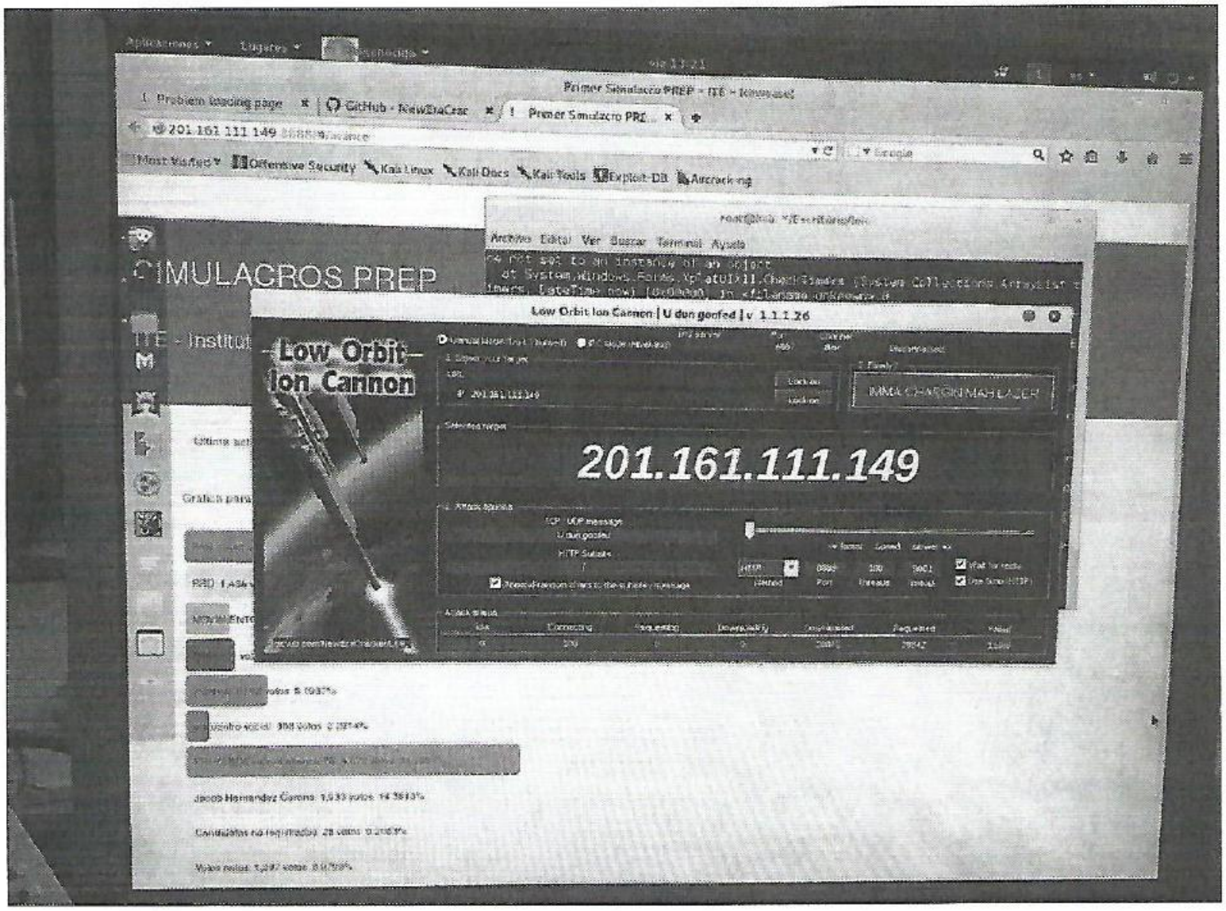
```
map -T4 -A -v 201.161.111.149
ompleted Ping Scan at 15:33, 0.24s elapsed (1 total hosts)
nitiating Parallel DNS resolution of 1 host. at 15:33
ompleted Parallel DNS resolution of 1 host. at 15:33, 0.72s
lapsed
nitiating SYN Stealth Scan at 15:33
canning 201.161.111.149 [1000 ports]
iscovered open port 21/tcp on 201.161.111.149
iscovered open port 1720/tcp on 201.161.111.149
Discovered open port 8888/tcp on 201.161.111.149
Discovered open port 3389/tcp on 201.161.111.149
SYN Stealth Scan Timing: About 36.30% done; ETC: 15:34 (0:00:54
remaining)
SYN Stealth Scan Timing: About 38.60% done; ETC: 15:35 (0:01:37
remaining)
Increasing send delay for 201.161.111.149 from 0 to 5 due to 12
out of 29 dropped probes since last increase.
SYN Stealth Scan Timing: About 41.80% done; ETC: 15:36 (0:02:07
remaining)
Completed SYN Stealth Scan at 15:34, 102.44s elapsed (1000 total
ports)
```

IMG2.- Validación de cierre de puertos servidor PREP Tlaxcala

Juan Carlos Olivares

Pruebas de Denegación de Servicios (DDOS)

Se realizaron pruebas de DDOS con la intención de garantizar que el servidor soportara un ataque de este tipo, para lo cual se utilizó un software llamado LOIC (Low Orbit Ion Cannon) el cual permite enviar una gran cantidad de paquetes o peticiones al servidor en un periodo de tiempo con la intención de verificar si este es capaz de soportar una carga excesiva de peticiones o es capaz de soportar la carga de trabajo. Una vez realizadas las pruebas se determinó que el servidor podría soportar una gran demanda de peticiones sin ningún problema.



```
is not set to an instance of an object
  at System.Windows.Forms.XplatUIX11.CheckTimers (System.Collections.ArrayList timers, DateTime now) [0x00000] in <filename unknown>:0
```

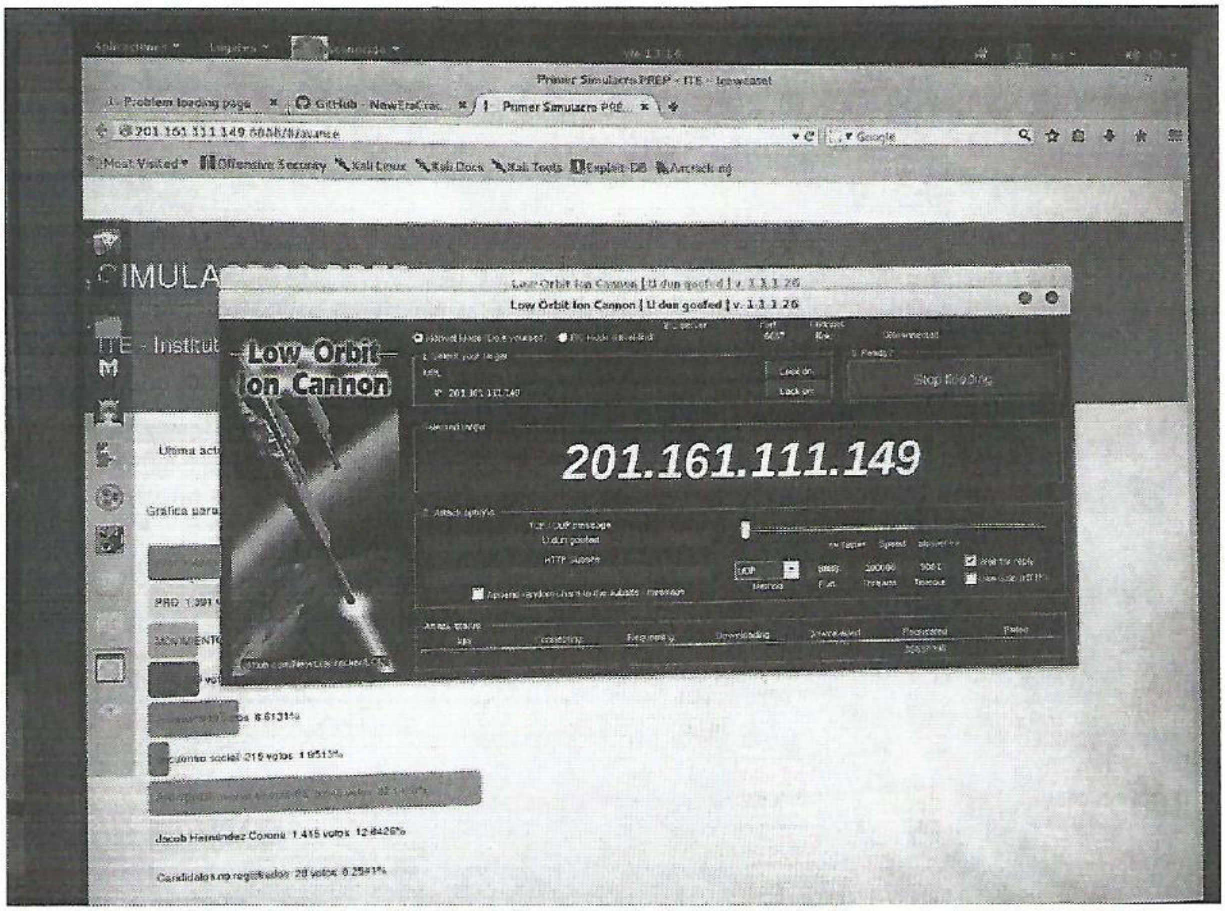
Jacob Hernandez Corona: 1,533 votos 14.3813%

Candidatos no registrados: 28 votos 0.2083%

Votos nulos: 1,297 votos

IMG3.- Prueba de DDOS con peticiones HTTP

Juan Carlos Olivares So



IP: 201.161.111.149

Method: UDP

PRD 1,391

MOVIMIENTO

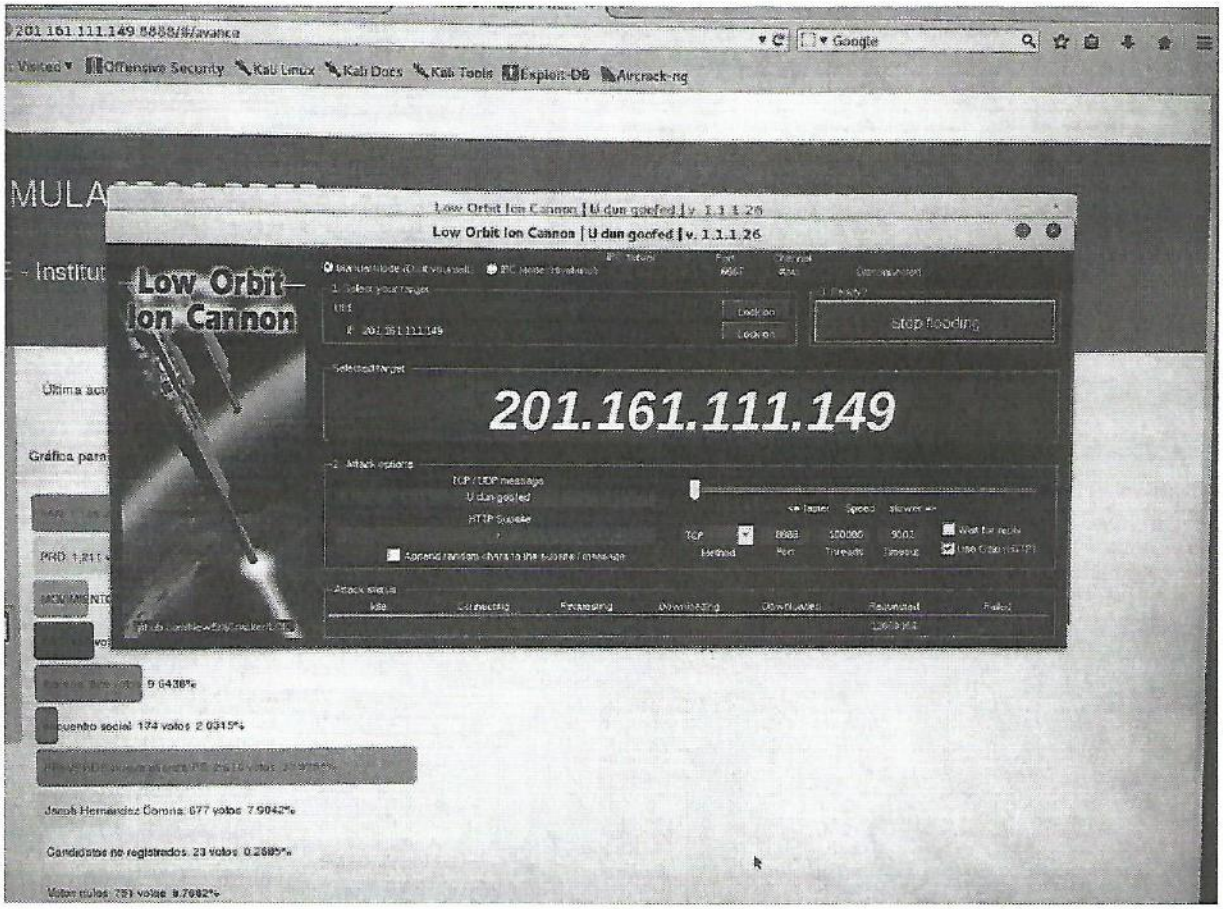
Encuentro social 215 votos 1.9513%

Jacob Hernández Corona 1,415 votos 12.8426%

Candidatos no registrados 28 votos 0.2541%

IMG3.- Prueba de DDOS con peticiones UDP

Juan Carlos Olivares



201.161.111.149:8888/#/avance

Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.26

IP: 201.161.111.149

Selected target: 201.161.111.149

TCP / UDP message: U dun goofed

Method: TCP · Port: 8888 · Threads: 100000 · Timeout: 9001

☑ Use Gzip (HTTP)

Encuentro social: 174 votos 2.0315%

Jacob Hernandez Corona: 677 votos 7.9042%

Candidatos no registrados: 23 votos 0.2685%

Votos nulos: 751 votos 8.7682%

IMG3.- Prueba de DDOS con peticiones TCP

Conclusiones

Después de realizar las pruebas anteriores se determinó que el servidor, donde se aloja el sistema PREP y el sistema de seguimiento, está protegido debidamente y es capaz de soportar una gran demanda de peticiones, por lo tanto es seguro y garantiza que los resultados que se mostraran al público serán resultados fieles a la captura de las actas de la elección.

Juan Carlos Olivares