



Act 3.4 - Actividad Integral de BST

Investigacion y reflexion

Programación de estructuras de datos y algoritmos fundamentales (Gpo 4)

Alumnos:

Thomas Freund Paternostro //A00831997

Fecha de entrega:

22/10/2021

La importancia y eficiencia del uso de BST en una situación problema de esta naturaleza

La importancia de un BST para poder tratar con una situación problema de esta naturaleza es que permite encontrar fenómenos y patrones por la misma naturaleza de la estructura de datos. En la bitácora que se trabajó se puede evidenciar las siguientes cinco y IPS con más acceso.

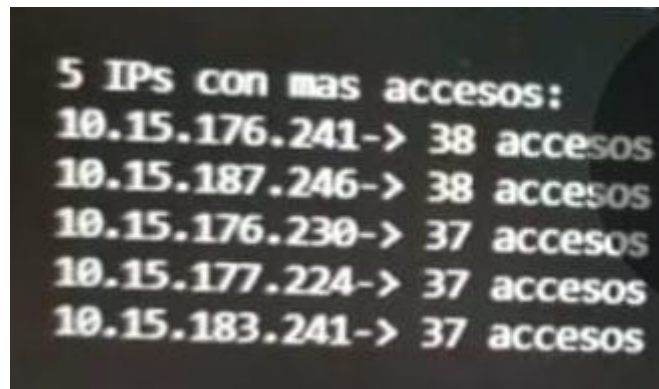


Imagen 1 - Las 5 IPs de la bitácora con más acceso

En la bitácora se puede hacer referencia a estos ipes y se puede evidenciar que las 5 y IPS con más accesos dan a usuarios ilegales que están tratando de entrar al sistema y estos son rechazados en los diferentes niveles de acceso.

```
Jun 2 22:24:15 10.15.173.220:4014 Illegal user
Jul 10 14:20:29 10.15.188.231:6314 Illegal user
Jun 25 15:31:01 10.15.185.252:5762 Failed password for illegal user guest
Oct 23 1:23:16 10.15.182.233:4640 Failed password for admin
Aug 21 19:32:57 10.15.170.247:4074 Failed password for illegal user guest
Jun 1 23:35:58 10.15.176.250:6009 Failed password for illegal user test
Sep 20 13:10:51 10.15.171.228:6300 Failed password for illegal user test
Jul 30 18:23:55 10.15.171.250:6353 Failed password for illegal user test
Oct 28 3:59:32 10.15.176.241:6550 Illegal user
Oct 11 11:26:43 10.15.184.237:5818 Failed password for illegal user guest
```

Imagen 2 - Primer IP con mayor acceso

```
Jun 2 0:57:36 10.15.173.248:6402 Failed password for root
Jun 28 12:33:03 10.15.185.225:6098 Failed password for root
Oct 2 9:52:21 10.15.187.246:5692 Illegal user
Oct 2 13:18:03 10.15.180.233:6391 Failed password for illegal user test
Jun 17 3:21:59 10.15.179.247:4436 Failed password for root
Jun 7 11:20:11 10.15.175.229:6086 Illegal user
```

Imagen 3 - Segundo IP con mayor acceso

```
Aug 28 14:12:11 10.15.176.230:4964 Illegal user
Sep 10 6:09:10 10.15.177.225:5836 Failed password for illegal user guest
Sep 3 22:04:01 10.15.181.246:6087 Failed password for root
Oct 23 2:13:28 10.15.182.246:6914 Failed password for illegal user guest
```

Imagen 4 - Tercero IP con mayor acceso

```
Oct 28 8:55:59 10.15.183.241:5300 Failed password for admin
Jun 24 17:48:16 10.15.186.220:5350 Failed password for root
Oct 21 20:26:05 10.15.176.238:5325 Failed password for root
Jun 1 13:11:31 10.15.178.252:6435 Failed password for illegal user guest
```

Imagen 4 - Cuarto IP con mayor acceso

En la IP 10.15.177.224 se trata ejemplificar a mayor profundidad este caso donde se puede evidenciar que en diferentes fechas el usuario trato de acceder al sistema dónde se lo detectó como usuario ilegal, trato y fracaso en poner una contraseña para el root y también fracasó en poner la contraseña para la cuenta de admin. En este caso hay 37 accesos y solo se ejemplifican tres pero cabe resaltar el comportamiento de los casos de ips más registrados en una bitácora dónde se registra la razón de porque no puedo entrar un usuario.

```
Sep 29 13:30:58 10.15.177.224:6144 Illegal user
Jun 26 15:47:27 10.15.180.221:4725 Illegal user
Aug 30 5:42:42 10.15.190.229:5550 Failed password for root
Aug 5 22:58:14 10.15.171.246:4037 Failed password for illegal user guest
Sep 14 3:20:39 10.15.185.242:6811 Failed password for illegal user test
```

```
Jul 10 5:09:04 10.15.177.224:5286 Failed password for root
Aug 29 11:04:57 10.15.184.242:4287 Failed password for illegal user test
Sep 16 2:13:28 10.15.180.235:4194 Illegal user
Oct 21 2:06:29 10.15.179.250:6834 Failed password for root
```

```
Jun 19 1:29:38 10.15.177.224:5636 Failed password for admin
Sep 21 13:05:19 10.15.182.228:5933 Illegal user
Sep 12 6:41:34 10.15.188.254:5580 Failed password for illegal user guest
Oct 16 9:01:29 10.15.183.220:6793 Failed password for root
```

Se considera que el método BST además de ser eficiente e importante en una situación problema con una naturaleza delicada como la presentada en esta actividad, también por las reglas de ordenamiento de la misma estructura de datos permite encontrar posibles vulnerabilidades en el sistema.

Otro punto que tiene que ser tomado a reflexión es que estos datos sin la interpretación humana que investigue y realmente ponga criterio el significado y las consecuencias de usuarios como estos. La importancia o eficiencia del BST no serviría dado que esta es una herramienta para poder tomar decisiones más no el único método.

¿Cómo podrías determinar si una red está infectada o no?

Según estudios casi un tercio de todos los ordenadores en el mundo se reportan tener algún tipo de malware. Donde no necesariamente sea posible evidenciar un equipo que está infectado pero la manera principal de detectarlo es con software anti-malware o spyware o cualquier tipo de software malicioso. Estos programas buscan en todo el ordenador y están desarrollados de tal manera que saben dónde buscar y encontrar la gran cantidad de archivos ya que hacen referencia seguramente a una o miles de bibliotecas para poder identificar posibles rastros o malwares presentes en un ordenador.

Como referencia en Estados Unidos 82% de las casas conectadas al internet tienen algún tipo de software antier según security.org. De esta estadística corresponde a 86 millones de casa que reportan utilizar este tipo de software y casi la mitad de ellos pagan por un servicio para proteger sus dispositivos. Por lo tanto en varios países desarrollados se pudiera estimar que se está tomando conciencia y por ende se asumirá que también en todo el mundo ya que es un tema de índole universal. Se considera que fuera de hacer chequeos constantes y verificar que todo el sistema esté funcionando correctamente con alguno de estos softwares o servicios es difícil no encontrar algún tipo de malware en un ordenador.

Referencias

EP Noticias. (2012, 8 octubre). *El 31,63 % de los ordenadores de todo el mundo está infectado con algún tipo de 'malware'* 20bits.

<https://www.20minutos.es/noticia/1610691/0/ordenadores/malware/virus/>

Security.org. (2021, 27 agosto). *Personal Antivirus Consumer Usage, Adoption & Shopping Study: 2021*.

[https://www.security.org/antivirus/antivirus-consumer-report-annual/#:%7E:text=Alo ng%20with%20awareness%2C%20usage%20is,free%20versions%20on%20the%20 market\).](https://www.security.org/antivirus/antivirus-consumer-report-annual/#:%7E:text=Alo ng%20with%20awareness%2C%20usage%20is,free%20versions%20on%20the%20 market).)