Universidad de los Andes

PROYECTO 2- ANALISIS DE TRAFICO
NICOLAS CAMILO MORENO ARIAS

1. Identifique todas las direcciones fuente y todas las direcciones destino.

Al analizar el tráfico de red, he observado un patrón intrigante relacionado con las direcciones fuente y destino. En el primer registro, pude identificar que la dirección fuente es 139.199.184.166 y su correspondiente dirección destino es 10.12.25.101. Sin embargo, en el segundo registro, se produjo un cambio en la disposición de estas direcciones. Ahora, la dirección destino del primer registro se convierte en la dirección fuente, es decir, 10.12.25.101, mientras que la dirección fuente del primer registro se convierte en la dirección destino, es decir, 139.199.184.166.

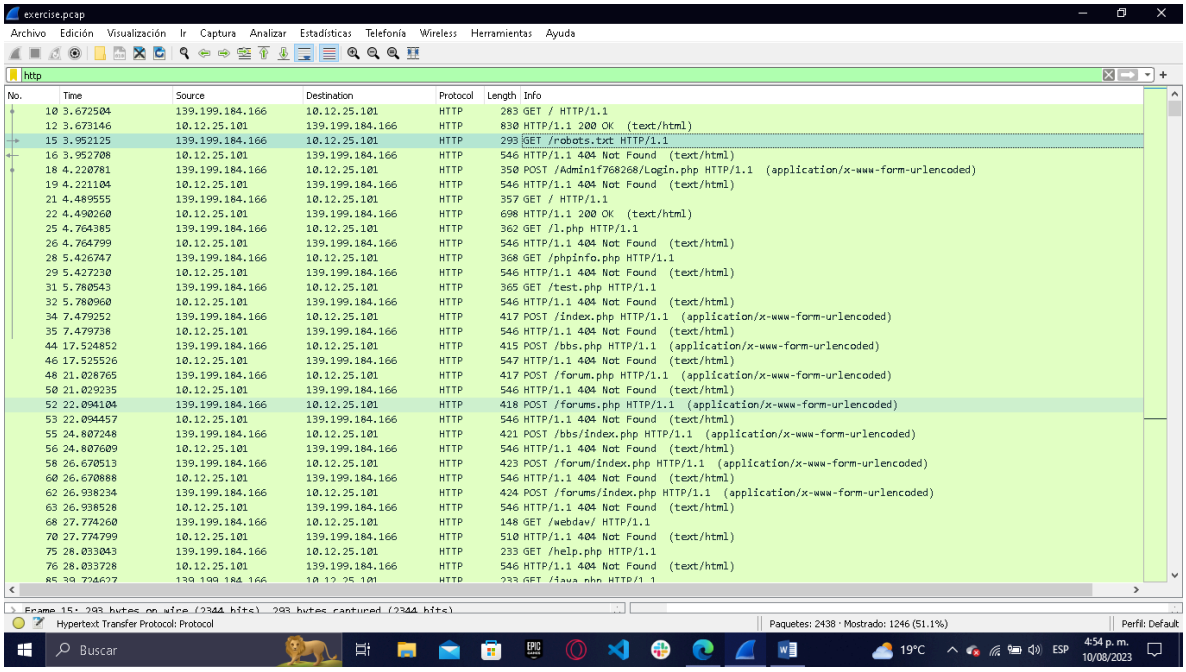
Este patrón de intercambio de direcciones se repite en los registros posteriores, como el tercero, el quinto y así sucesivamente. Estos cambios plantean preguntas intrigantes sobre la lógica detrás de la configuración de la red y su comportamiento. Podría indicar un diseño específico de la red con fines particulares o quizás esté relacionado con algún proceso automatizado que modifica las direcciones en cada registro por alguna razón en particular. Aquí podemos ver una imagen.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	139.199.184.166	10.12.25.101	TCP	62	55376 → 80 [SYN] Seq=0 Win=8192 Len=0 WS=256 SACK_PERM
2	0.000086	10.12.25.101	139.199.184.166	TCP	66	80 → 55376 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=1024
3	1.295311	139.199.184.166	10.12.25.101	TCP	60	55376 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	1.295354	139.199.184.166	10.12.25.101	TCP	60	55376 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131072 Len=0
5	1.295671	10.12.25.101	139.199.184.166	TCP	54	80 → 55376 [FIN, ACK] Seq=1 Ack=2 Win=29696 Len=0
6	1.562685	139.199.184.166	10.12.25.101	TCP	60	55376 → 80 [ACK] Seq=2 Ack=2 Win=131072 Len=0
7	3.404851	139.199.184.166	10.12.25.101	TCP	62	55812 → 80 [SYN] Seq=0 Win=8192 Len=0 WS=256 SACK_PERM
8	3.404946	10.12.25.101	139.199.184.166	TCP	66	80 → 55812 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=1024
9	3.672453	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
10	3.672504	139.199.184.166	10.12.25.101	HTTP	283	GET / HTTP/1.1
11	3.672579	10.12.25.101	139.199.184.166	TCP	54	80 → 55812 [ACK] Seq=1 Ack=230 Win=30720 Len=0
12	3.673146	10.12.25.101	139.199.184.166	HTTP	830	HTTP/1.1 200 OK (text/html)
13	3.940236	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=230 Ack=537 Win=131072 Len=0
14	3.940275	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=230 Ack=777 Win=131072 Len=0
15	3.952125	139.199.184.166	10.12.25.101	HTTP	293	GET /robots.txt HTTP/1.1
16	3.952708	10.12.25.101	139.199.184.166	HTTP	546	HTTP/1.1 404 Not Found (text/html)
17	4.219994	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=469 Ack=1269 Win=131072 Len=0
18	4.220781	139.199.184.166	10.12.25.101	HTTP	350	POST /Admin1f768268/Login.php HTTP/1.1 (application/x-www-form-urlencoded)
19	4.221104	10.12.25.101	139.199.184.166	HTTP	546	HTTP/1.1 404 Not Found (text/html)
20	4.488488	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=765 Ack=1761 Win=130816 Len=0
21	4.489555	139.199.184.166	10.12.25.101	HTTP	357	GET / HTTP/1.1
22	4.490260	10.12.25.101	139.199.184.166	HTTP	698	HTTP/1.1 200 OK (text/html)
23	4.757563	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=1068 Ack=2297 Win=131072 Len=0
24	4.757617	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=1068 Ack=2405 Win=131072 Len=0
25	4.764385	139.199.184.166	10.12.25.101	HTTP	362	GET /l.php HTTP/1.1
26	4.764799	10.12.25.101	139.199.184.166	HTTP	546	HTTP/1.1 404 Not Found (text/html)
27	5.032043	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=1376 Ack=2897 Win=131072 Len=0
28	5.426747	139.199.184.166	10.12.25.101	HTTP	368	GET /phpinfo.php HTTP/1.1
29	5.427230	10.12.25.101	139.199.184.166	HTTP	546	HTTP/1.1 404 Not Found (text/html)
30	5.694439	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=1690 Ack=3389 Win=130816 Len=0

2. Qué cree que está ocurriendo?

Creo que estamos observando una transferencia de diferentes documentos entre las mismas direcciones, lo cual me intriga por varias razones. Algunos de los registros muestran errores "404 Not Found", y también se hace mención de "robot.txt". Además, noto un registro en la sección de información que hace referencia a "test.txt". Esto me lleva a considerar la posibilidad de que estemos frente a un intento de ataque.

Es posible que el equipo de seguridad esté investigando si estas acciones señalan una vulnerabilidad en nuestros componentes o si estamos siendo blanco de un ataque coordinado. También podría ser que la actividad relacionada con "test.txt" sea parte de una rutina de verificación para asegurar el correcto funcionamiento del sistema.



En conclusión, en mi opinión, parece que estamos siendo objeto de un ataque, ya que se han presentado múltiples avisos de error 404 de manera inconsistente.

Gracias por leer