SOC176 - RDP Brute Force Detected

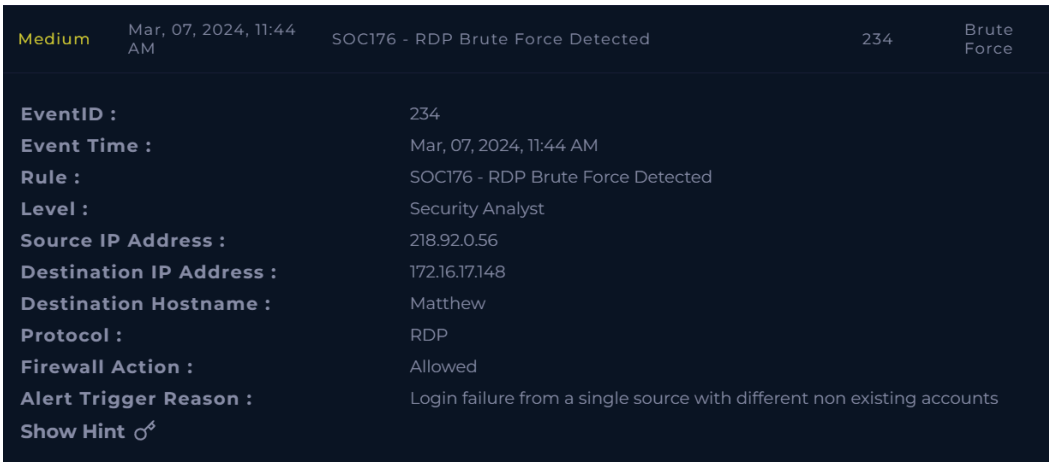
Contenido

Descripción

El 07 de marzo de 2024, a las 11:44 AM, se recibió una alerta donde se observa un intento de fuerza bruta RDP (Remote Desktop Protocol), el objetivo es determinar si se trata de un verdadero o falso positivo comprobando si el acceso fue exitoso. Un intento de fuerza bruta RDP exitoso puede llevar a un acceso no autorizado a sistemas críticos, exponiendo información confidencial, comprometiendo la integridad del entorno y permitiendo la ejecución de acciones maliciosas, como la instalación de malware o el robo de datos.

Contexto: Remote Desktop Protocol (RDP) es una tecnología que permite a los usuarios conectarse de manera remota a otros dispositivos, accediendo a escritorios y aplicaciones desde diferentes ubicaciones. Aunque sigue siendo ampliamente utilizado en 2024, especialmente en entornos corporativos y de soporte técnico, su seguridad ha sido puesta en duda debido a vulnerabilidades que lo hacen un blanco frecuente de ciberataques, como los intentos de fuerza bruta. A pesar de estos riesgos, RDP sigue siendo relevante, aunque su uso requiere configuraciones de seguridad robustas.

Detalles de la alerta

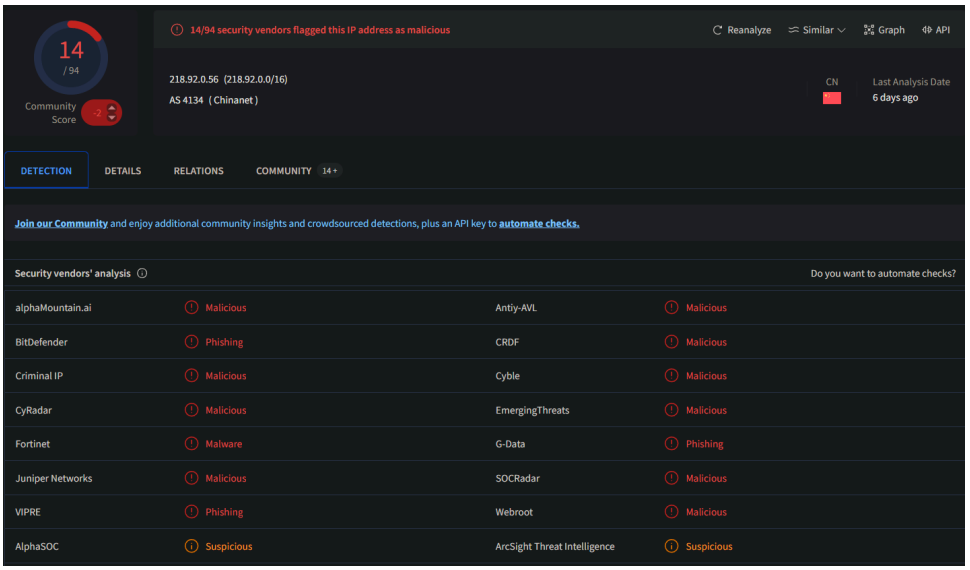


- **ID de evento**: 234
- **Tiempo del evento**: Mar, 07, 2024, 11:44 AM
- **Type**: Brute Force
- **Subtype**: Brute Force (Remote Desktop Protocol)
- **Regla**: SOC176 - RDP Brute Force Detected
- **Source IP Address:** 218[.]92[.]0[.]56
- **Destination IP Address:** 172[.]16[.]17[.]148
- **Destination Hostname:** Matthew
- **Protocol**: RDP
- **Firewall Action:** Allowed
- **Alert Trigger Reason:** Login failure from a single source with different non existing accounts

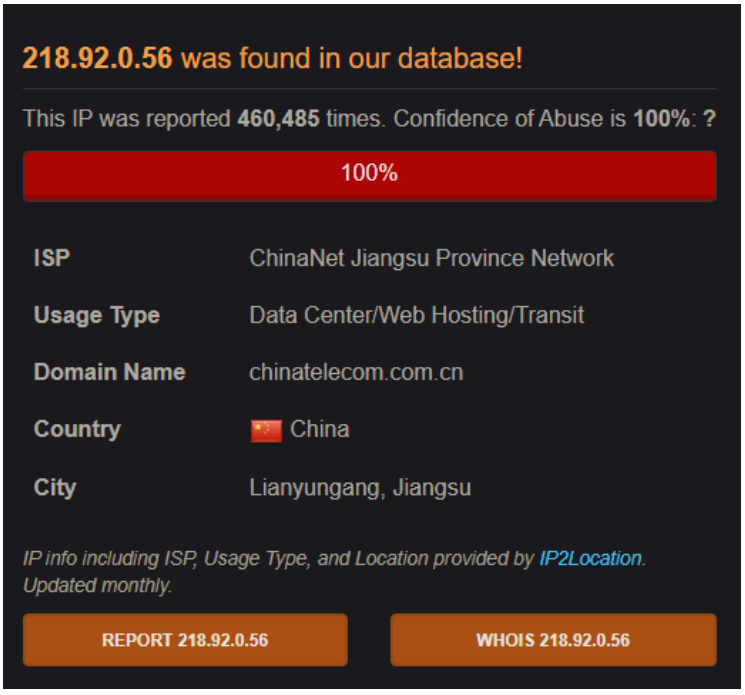
Análisis

Lo primero que observamos es que la IP de origen (218[.]92[.]0[.]56) es externa por lo que se procede a utilizar herramientas correspondientes para su análisis.

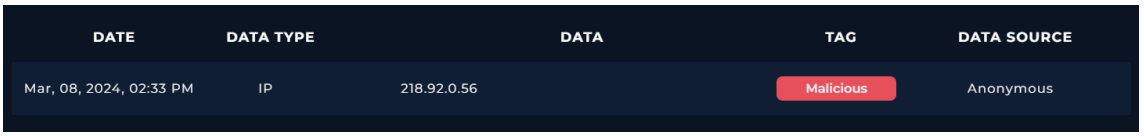
- Virustotal



- AbuseIPDB



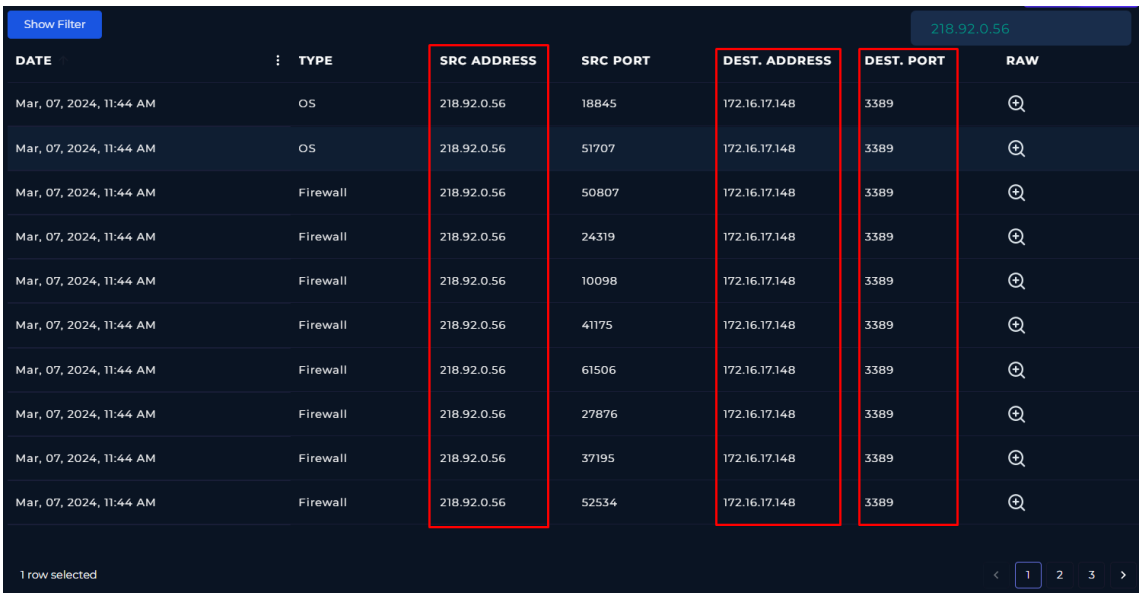
- Threat Intelligence de LestDefend

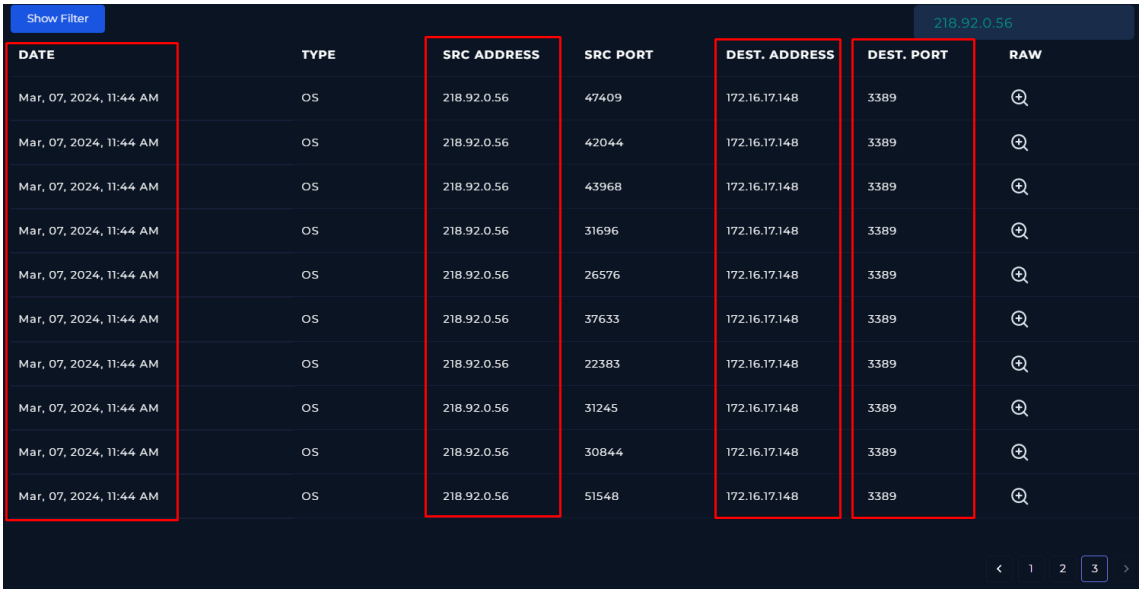


Una vez comprobado que se trata de una IP maliciosa debemos registrar todas las interacciones que tuvo con el sistema y si verdaderamente pudo concretar el ataque de fuerza bruta o fue bloqueado.

Principalmente debemos buscar si existen solicitudes de la dirección IP del atacante al puerto SSH o RDP del servidor de destino.

Para esto utilicé la herramienta de Log Management de LetsDefend filtrando registros que contengan la IP maliciosa. Como resultado obtenemos 3 secciones de logs del mismo día a la misma hora hacia la misma IP (172[.]16[.]17[.]148) y puerto objetivo (3389) que justamente es el puerto utilizado para RDP.





Revisando cada uno de los registros identificamos los siguientes usuarios involucrados utilizados para realizar fuerza bruta :

- admin
- sysadmin
- guest
- Matthew

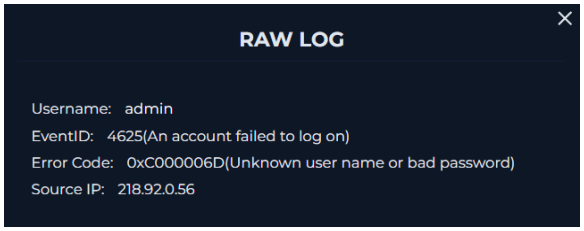
Analizando los códigos de error, los usuarios **admin**, **sysadmin y guest** no existen ya que cuando se intenta con **Matthew** pero la contraseña es incorrecta son distintos códigos de error y este nos da un indicio de que el usuario Matthew existe.

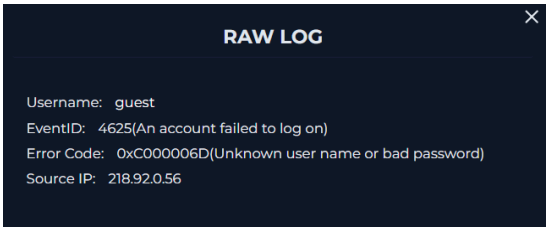
Intentos de inicio de sesión incorrectos:

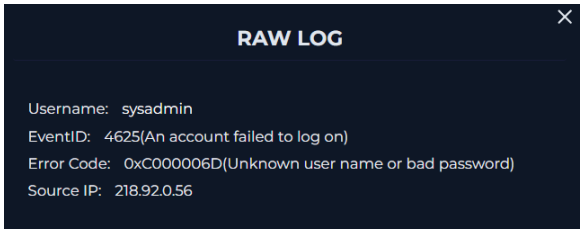
EventID: 4625<- Es importante esta información que nos da el registro de log ya que es un identificador de seguridad de Windows relacionado con intentos de autenticación. Muy utilizado en filtros para detectar intentos de fuerza bruta.

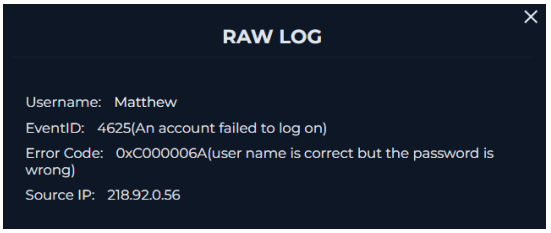
Detalles clave de Event ID 4625:

- **Account Name:** Nombre de la cuenta que intentó iniciar sesión.
- **Logon Type:** Indica el tipo de inicio de sesión (por ejemplo, remoto o local).
- **Failure Reason:** Razón por la cual falló el intento (credenciales incorrectas, cuenta inexistente, etc.).
- **Source Network Address:** La IP desde la que se intentó el inicio de sesión.







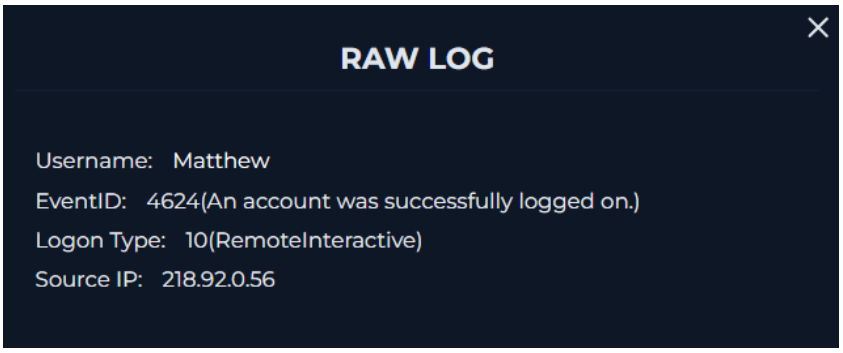


Inicio de sesión correcto:

EventID: 4624 <- Igual que el EventID 4625 es un identificador de seguridad de Windows relacionado con intentos de autenticación. En nuestro caso nos indica que en combinación por la gran cantidad de EventID 4625 registrados el intento de fuerza bruta fue exitoso.

Detalles clave de Event ID 4624:

- **Account Name:** Nombre de la cuenta que logró iniciar sesión.
- **Logon Type:** Tipo de inicio de sesión (puede ser remoto, local, etc.).
- **Source Network Address:** IP desde donde se originó el inicio de sesión exitoso.

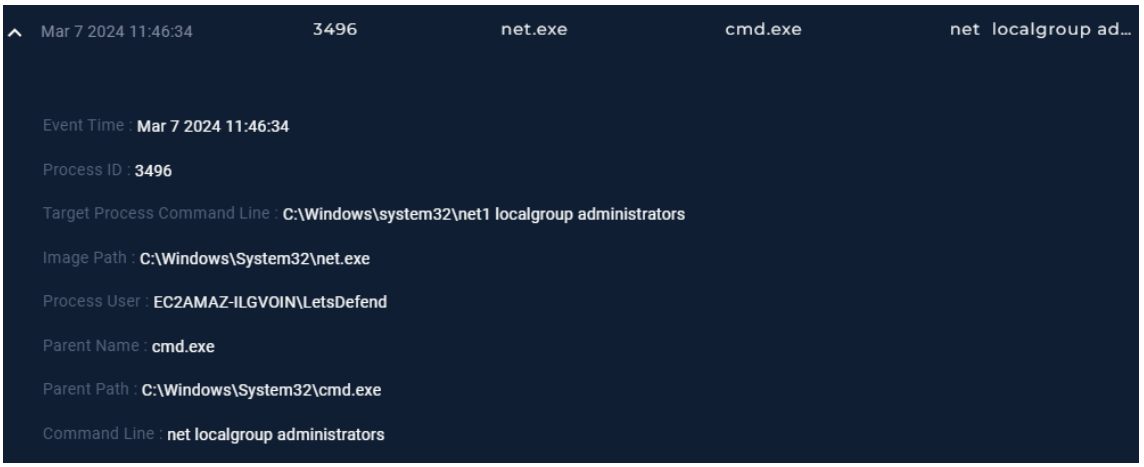


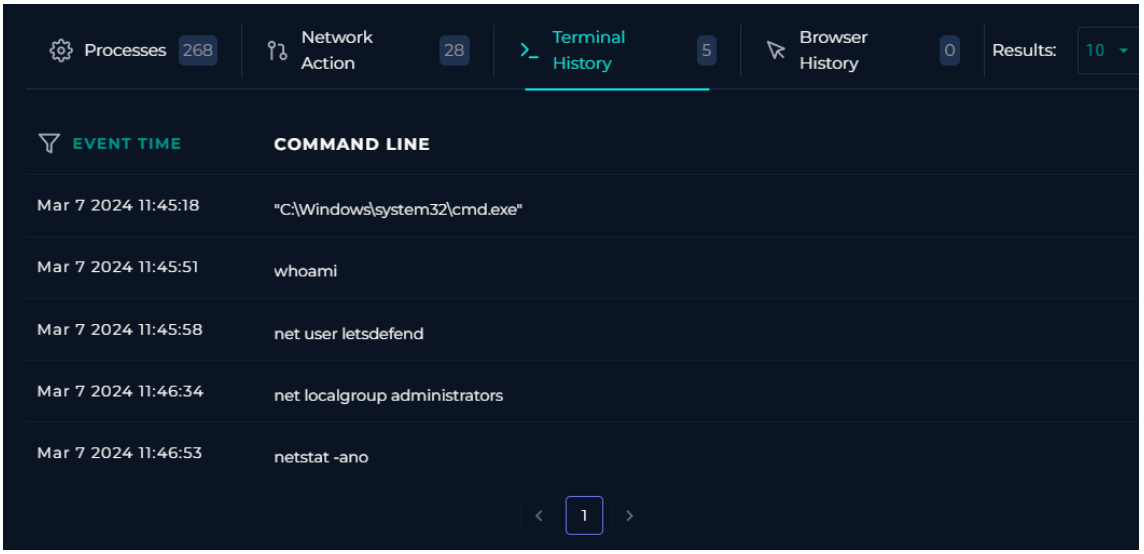
<u>En Linux podemos ver estos “eventos”:</u>

- cat /var/log/auth.log | grep "Failed password" - cat /var/log/auth.log | grep "Accepted password

Sin embargo es importante destacar que solo la dirección IP del atacante intenta establecer una conexión SSH/RDP un único objetivo (172[.]16[.]17[.]148)

Al revisar procesos y comandos ejecutados por el host Matthew se observa que se ejecuta un CMD con una serie de ejecuciones de comandos, incluidos intentos de recopilar información del sistema y escalar privilegios

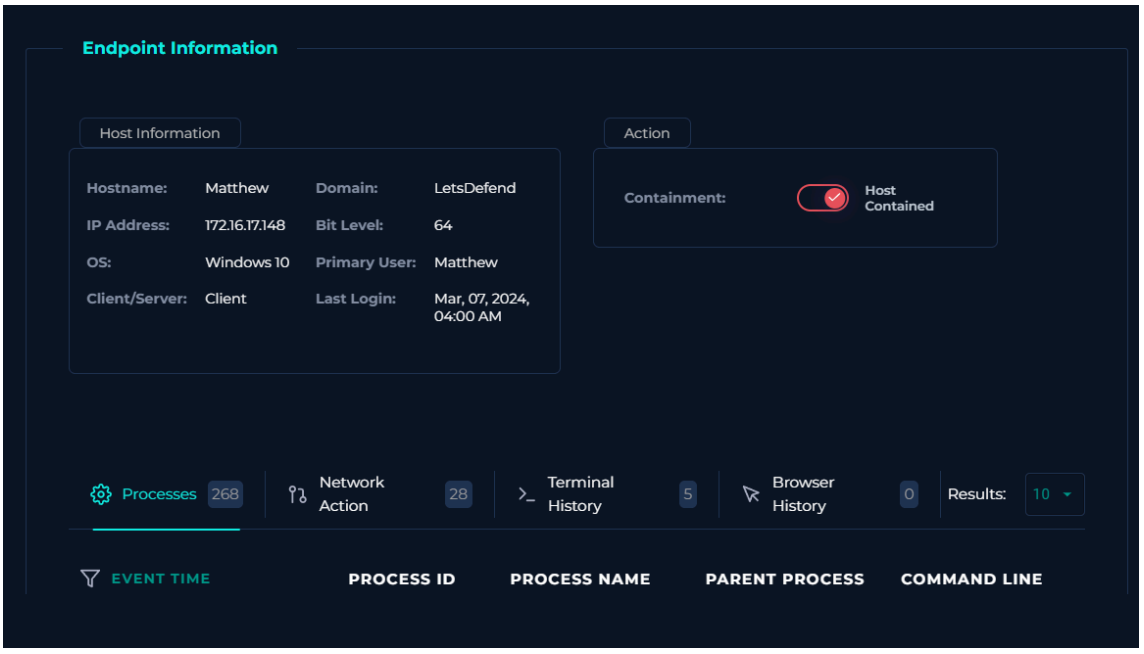




Respuesta

1. **Aislar la máquina afectada para evitar movimiento lateral.**

Esto mismo lo podemos realizar utilizando el Endpoint Security de LetsDefend



Recomendaciones

Las siguientes recomendaciones a implementar se dan con el fin de prevenir futuros ataques de la misma naturaleza.

1. **Implementar Autenticación Multifactor (2MFA o MFA)**

La autenticación multifactor es una de las medidas más efectivas para proteger accesos remotos. Incluso si un atacante consigue la contraseña correcta, sin el segundo factor (como un token, aplicación de autenticación o biometría), no podrá acceder.

2. **Restringir el Acceso RDP a Nivel de Red**

Limitar IPs de acceso: Configurar listas de control de acceso (ACLs) o reglas de firewall para restringir las IPs que pueden conectarse a través de RDP. Solo direcciones IP específicas (como las de la VPN o ubicaciones seguras) deberían tener acceso.

VPN obligatoria: Exigir que las conexiones RDP solo se realicen a través de una VPN segura, evitando exponer directamente RDP a Internet.

3. **Políticas de Bloqueo de Cuenta (Account Lockout Policies)**

Configurar políticas de seguridad para bloquear temporalmente las cuentas después de un número determinado de intentos fallidos de inicio de sesión. Esto previene ataques de fuerza bruta, ralentizando al atacante significativamente.

4. **Fortalecer la Configuración del Protocolo RDP**

Usar cifrado fuerte: Asegurarse de que RDP esté configurado con las opciones de cifrado más seguras.

Desactivar RDP si no es necesario: Si RDP no es esencial en ciertos servidores o usuarios, desactivarlo para reducir la superficie de ataque.

5. **Monitoreo y Alerta de Actividades Sospechosas**

Herramientas de monitoreo (SIEM) para detectar patrones de fuerza bruta y generar alertas tempranas. Monitorear intentos fallidos repetidos, accesos desde IPs inusuales y cualquier actividad anómala en sesiones RDP.

6. **Políticas de Contraseñas**

Revisar las contraseñas de las cuentas para asegurarse de que sean robustas y no reutilizadas en otros sistemas. Uso de contraseñas complejas.

Rotación de contraseñas: Forzar el cambio de contraseñas para las cuentas comprometidas o aquellas que fueron blanco del ataque.

7. **Auditoría de Seguridad y Parches**

Realizar una auditoría de seguridad completa de la máquina comprometida para detectar y eliminar posibles malware o puertas traseras.

Actualizar y aplicar parches tanto al sistema operativo como al protocolo RDP, asegurándose de que no haya vulnerabilidades conocidas que puedan ser explotadas.

Conclusiones

Se determinó luego de analizar los registros de logs que se realizó un ataque de fuerza bruta a través de RDP utilizando los siguientes usuarios: admin, sysadmin, guest y Matthew. Este último logró ser vulnerado por la fuerza bruta, resultando en un acceso exitoso. El ataque fue lanzado desde la dirección IP externa 218.92.0.56, la cual está clasificada como maliciosa en múltiples plataformas de inteligencia de amenazas. El análisis posterior reveló una serie de ejecuciones de comandos, incluidos intentos de recopilar información del sistema y escalar privilegios.