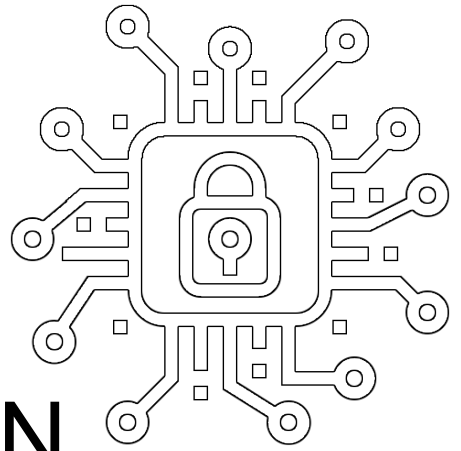


EXAMEN TRANSVERSAL

Bastian Fierro – Daniel Santibañez – Tamar Andrade

AGENDA

Introducción

Identificación de vulnerabilidades

Explotación de vulnerabilidades

Plan de mitigacion

Desarrollo politica

Lecciones Aprendidas

Conclusión

INTRODUCCIÓN

Como parte del equipo de la empresa Pretorian, nos contrataron para realizar una revisión de las políticas de seguridad en la empresa Saam S.A.

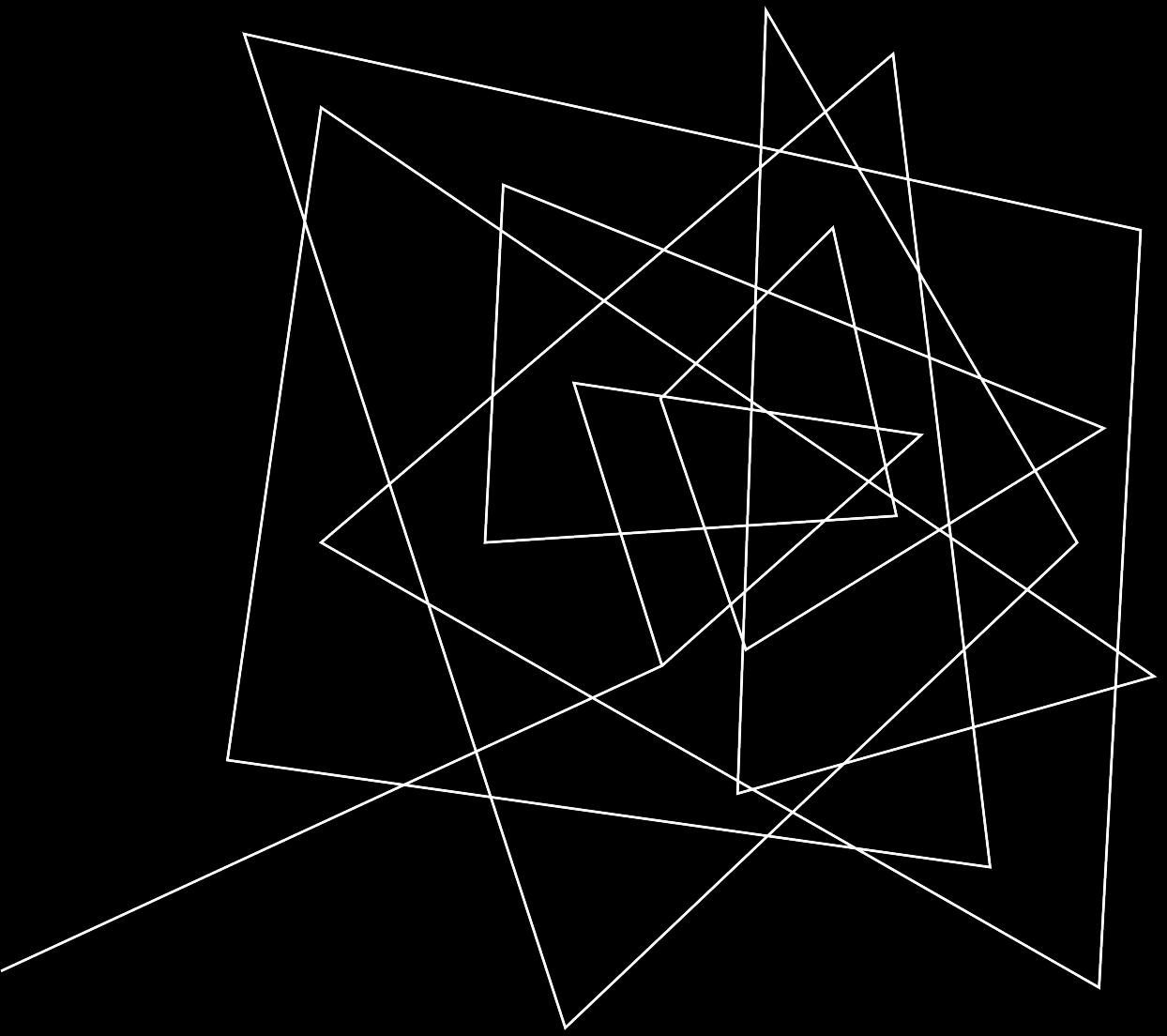
La compañía tiene la inquietud del robo de información en la base de datos de un servidor que actualmente aloja el portafolio de clientes de la empresa. En este contexto, se nos solicitó realizar una auditoría con el objetivo de alcanzar el hosting, en donde se almacena la base de datos.

Las condiciones que la empresa propone son:

No será proporcionado acceso a la red de manera formal.

El equipo debe identificar el hosting dentro de la red.

El equipo debe identificar las vulnerabilidades dentro del entorno.



IDENTIFICACIÓN DE VULNERABILIDADES

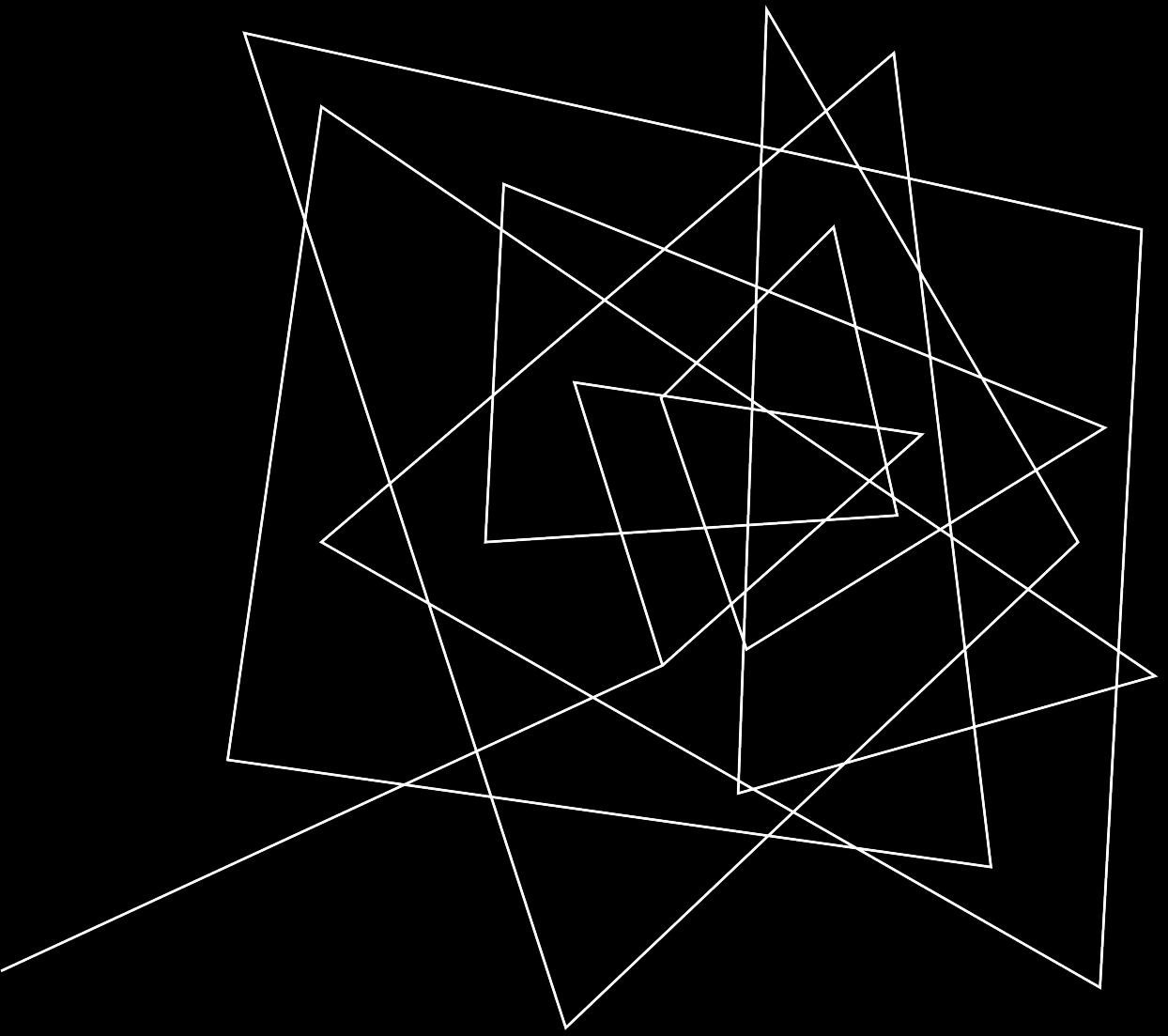
IDENTIFICACIÓN DE VULNERABILIDADES

Como equipo nos dimos cuenta de varias vulnerabilidades al ingresar a la empresa para realizar la auditoria.

Estas Vulnerabilidades podrían ser explotadas por algún intruso o atacante. Alguna de las vulnerabilidades que observamos son:

- Insuficiente control de acceso físico en las instalaciones (información personal a la vista).
- Red de Wifi Abierta.
- La ausencia de una política de gestión de contraseñas.
- Un puerto vulnerable abierto (UPNP).

Por eso es clave conocer e identificar a tiempo para implementar controles y hacer ajustes necesarios que permitan eliminar estas debilidades.



EXPLOTACIÓN DE VULNERABILIDADES

EXPLOTACIÓN DE VULNERABILIDADES

Algunas vulnerabilidades ponen en riesgo la seguridad del sistema. Estos pueden ser utilizado por algún ciber atacante para infiltrarse en el sistema de una victima y robar información confidencial para la empresa.

Para el caso ya sabiendo nuestra IP privada, ejecutamos el comando ‘nmap -sP 192.168.X.*’, para escanear todos los equipos encendidos conectados a la red local.

Luego, analizamos los nombres definidos de cada máquina, y con lógica, encontramos un patrón repetitivo como nombre de varias máquinas (el nombre por defecto de los equipos en la oficina, con la sigla ‘LC’), y había una máquina que se diferenciaba del resto, porque tenía un nombre de computadora personal (Desktop-XXXXXX), y decidimos empezar por este equipo.

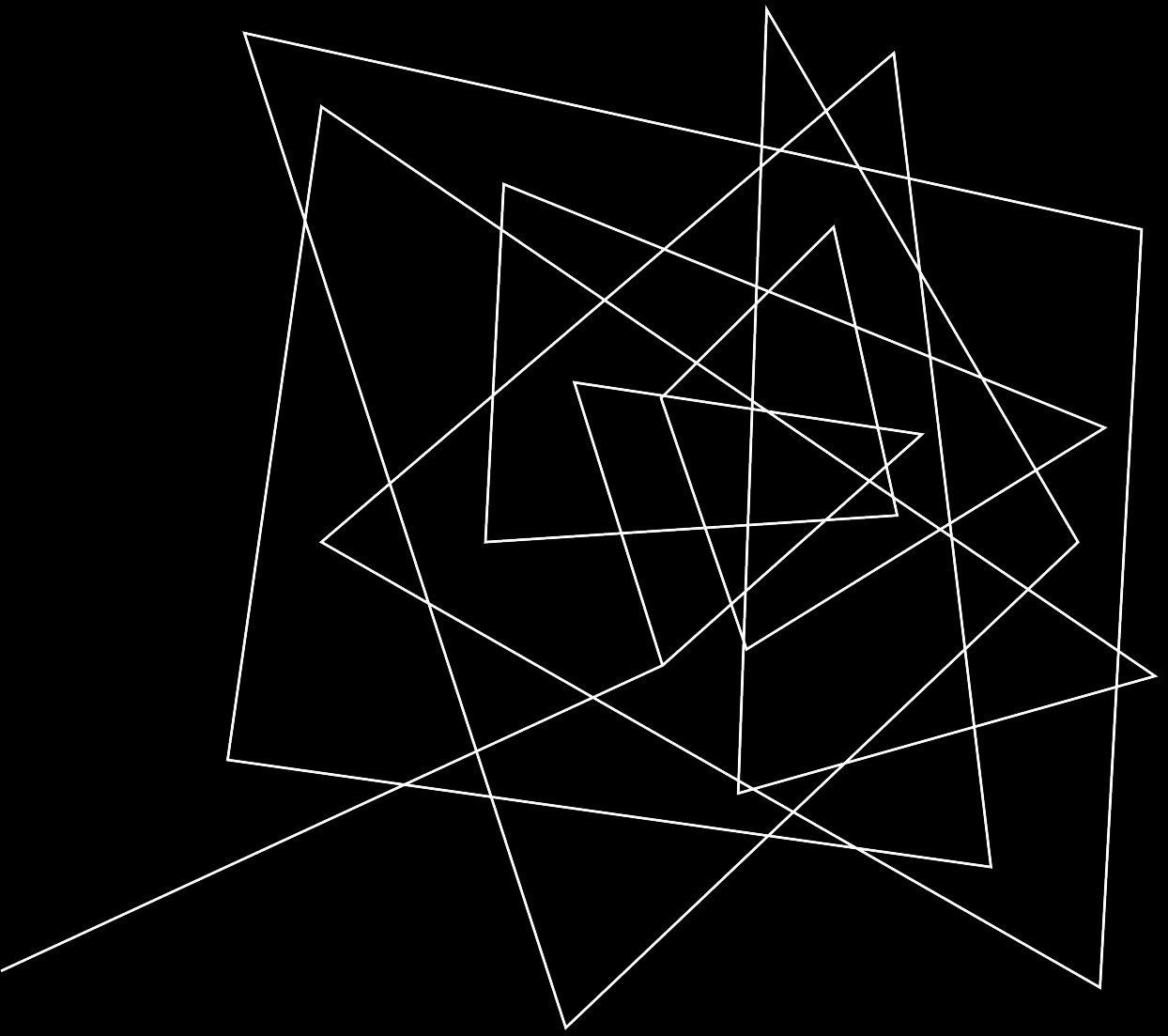
EXPLOTACIÓN DE VULNERABILIDADES

Guardamos el IP local de esta máquina, y la escaneamos con el comando ‘nmap -v -sV -O 192.168.X.X’, para ver detalles del escaneo, su sistema operativo y sus servicios.

Una vez confirmado que esta es la máquina objetivo, analizamos los servicios que tiene para ver sus puertos y encontrar uno vulnerable. En este caso, nos fijamos que el servicio UPNP con el puerto 5000 estaba abierto, el cual es vulnerable porque este servicio básicamente le habilita la entrada a cualquier dispositivo asumiendo que viene de una conexión confiable y local.

Luego, tenemos 2 opciones, usar el comando ‘telnet 192.168.X.X 5000’, o ingresar con PuTTY, seleccionando una conexión de tipo telnet, con la IP de la máquina y el puerto vulnerable.

Y la conexión con la máquina fue establecida sin pedir ni usuario ni contraseña para acceder a la consola.



PLAN DE MITIGACIÓN

PLAN DE MITIGACIÓN

Es importante para la entidad implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente, y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información. En la fase de contención busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI, para facilitar esta tarea la entidad debe poseer una estrategia de contención previamente definida para poder tomar decisiones, por ejemplo: apagar sistema, desconectar red, deshabilitar servicios.

Contención: Evitar que el incidente siga produciendo daño.

Erradicación: Eliminar la causa del incidente y rastros del daño.

Recuperación: Volver el entorno afectado a su estado original.

PLAN DE CONTENCIÓN

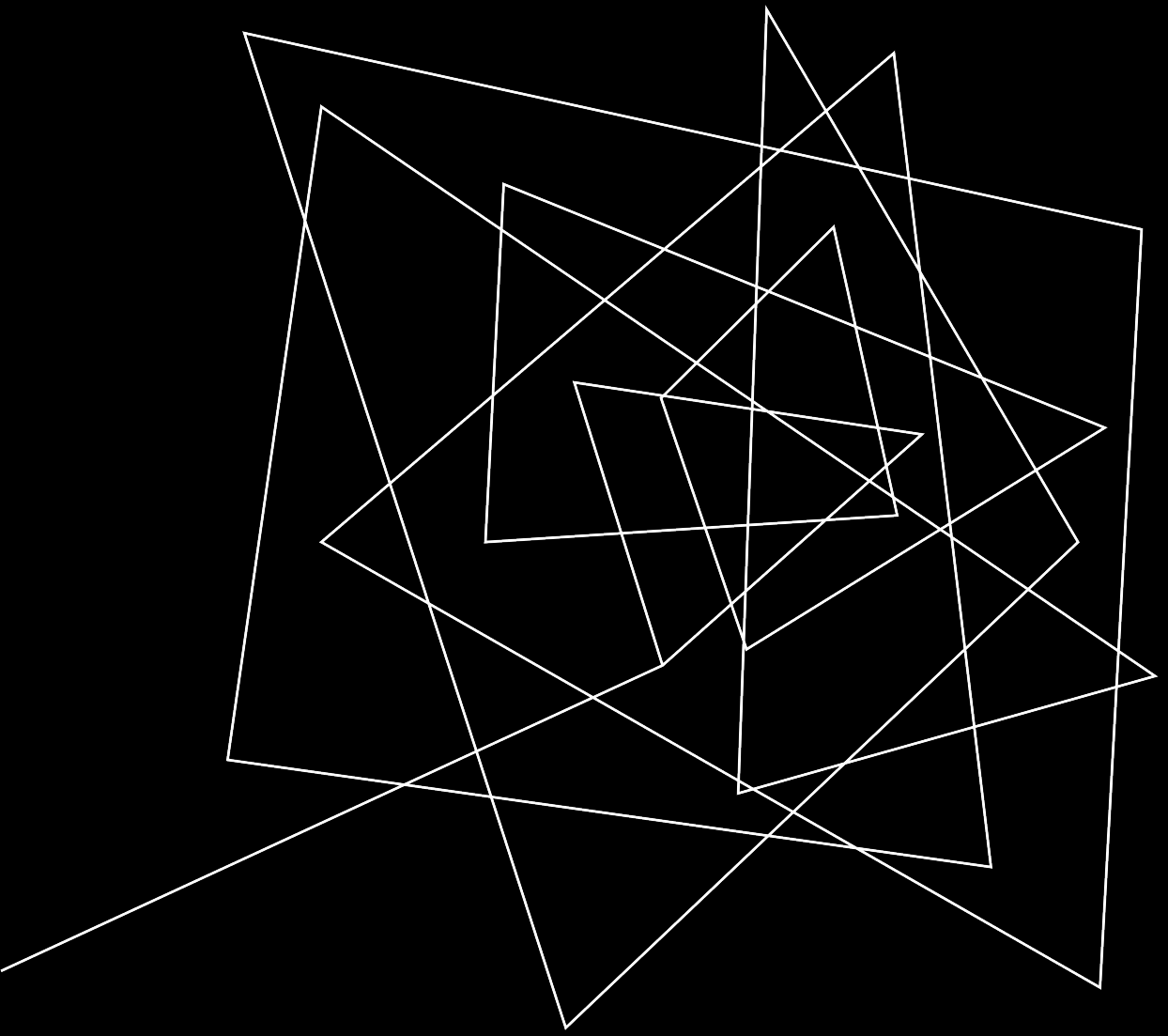
ID	Incidente	Ejemplo	Estrategia de contención
I1	Intento de acceso fallido	Multiples intentos fallidos de ingreso	Bloqueo de Cuenta
I2	Programa Malicioso	Infección con Virus	Aislar equipo de la red.
I3	Vulneración	Servidor principal vulnerado	Apagar el servidor principal y levantar un servidor espejo
I4	DoS	Servidor principal atacado con denegación de servicio	Bloquear o redirigir los paquetes del ataque
I5	Reconocimiento	Escaneo de puertos	Identificación y cierre de puertos

PLAN DE ERRADICACIÓN

ID	Incidente	Ejemplo	Estrategia de Erradicación
I1	Intento de acceso fallido	Multiples intentos fallidos de ingreso	Notificar al dueño de la cuenta para que restaure su cuenta
I2	Programa Malicioso	Infección con Virus	Ejecutar el antivirus de la maquina
I3	Vulneración	Servidor principal vulnerado	Redirigir al atacante a un Honeypot
I4	DoS	Servidor principal atacado con denegación de servicio	Contactar al proveedor del servicio de internet
I5	Reconocimiento	Escaneo de puertos	Incorporación de reglas de filtrado en el firewall

PLAN DE RECUPERACIÓN

ID	Incidente	Ejemplo	Estrategia de contención
I1	Intento de acceso fallido	Multiples intentos fallidos de ingreso	Activación de la cuenta
I2	Vulneración	Servidor principal vulnerado	Restaurar la información del servidor con un respaldo
I3	Acceso no deseado	Acceso no deseado a la red Wifi	Cambiar la contraseña de la red
I4	DoS	Servidor principal atacado con denegación de servicio	Volver el servicio al estado original.
I5	Programa Malicioso	Infección con Virus	Restaurar la información de la maquina con un respaldo



DESARROLLO DE POLITICAS

DESARROLLO DE POLITICAS

- Política de Gestión de usuarios y contraseñas.
  - Objetivo : Establecer los lineamientos para la adecuada asignación y uso de las cuentas de usuarios y contraseñas.
  - Alcance: Todas las cuentas de usuarios y contraseñas utilizadas en los sistemas y aplicaciones existentes.
  - Responsables: Personal de la empresa es responsable por cumplir con lo establecido en la presente política (Encargado de TI, en conjunto con el Encargado de Ciberseguridad y/o Seguridad de la Información.).

ALGUNAS POLÍTICAS SON:

- Los usuarios y contraseñas asignados al personal del organismo son personales e intransferibles.
- El personal de la empresa es responsable de la actividad asociada a su usuario. La empresa debe registrar la actividad de los usuarios, para su posterior control en caso de ocurrencia de incidentes.
- Las contraseñas deben requerir cierto nivel de complejidad mínimo y no pueden estar asociadas a datos personales que permitan su deducción, como, por ejemplo: nombres propios, nombre de usuario, números de documento, dirección, teléfono, etc.
- Las contraseñas mínimamente deben cumplir con los siguientes requerimientos:
- Longitud mínima de 8 caracteres,
- Estar formada por al menos 3 características de las siguientes:
- caracteres alfabéticos mayúsculas
- caracteres alfabéticos minúsculas
- caracteres numéricos
- caracteres especiales o extendidos

ALGUNAS POLÍTICAS SON:

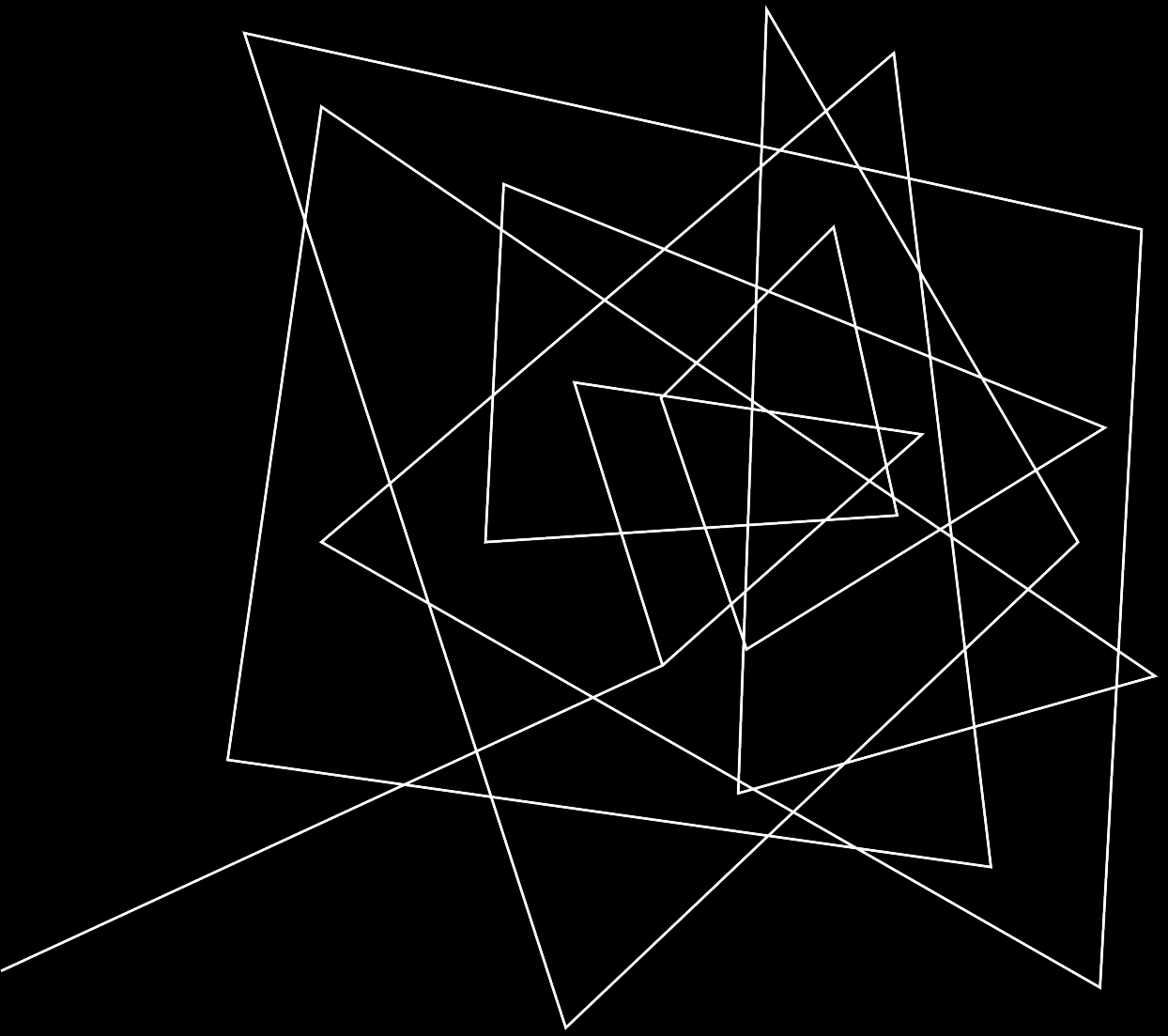
- La validez de las contraseñas no podrá superar los 3 meses. Dependiendo de la criticidad del sistema de información al cual se accede, se deberá manejar periodos más acotados.

  Se debe:

- Forzar al usuario a cambiar su contraseña en su primer uso y/o luego de ser asignada por un administrador de sistema.
- Realizar el bloqueo de la cuenta luego de reiterados intentos fallidos de inicio de sesión.
- Garantizar que el almacenamiento y la transmisión de las contraseñas de usuario se realizan de forma segura, de manera tal que los administradores de sistemas o todo aquel que cuente con usuario privilegiado, no tenga acceso a las mismas.

Algunas políticas que puedan estar relacionadas son:

- Política de control de acceso
- Política de gestión de usuarios de acceso privilegiado.
- Política de Registro y auditoria de eventos.



LECCIONES APRENDIDAS

LECCIONES APRENDIDAS

Con esta experiencia, generamos la siguiente lista de estrategias para prevenir este tipo de ataques a futuro:

Activar el firewall para proteger las redes privadas del acceso no autorizado y no verificado en una conexión a Internet.

Desactivar el servicio UPnP para evitar que cualquier persona acceda a la máquina.

Tener una política de contraseñas seguras, de manejo adecuado de los equipos y de la información.

Proteger la contraseña, cambiándola de forma periódica y que no esté visible de forma pública, para aumentar la seguridad de la red.

Generar logs de todas las actividades en el servidor para tener un control de toda actividad.

Escanear periódicamente los puertos de la red para evitar que servicios vulnerables estén activados.

Que el acceso esté limitado de acuerdo con el principio de privilegio mínimo.

Concientizar y capacitar frecuentemente a todos los empleados en buenas prácticas del uso de la información, así como en informar oportunamente sobre acciones y comportamientos fuera de lo común que pueden poner en riesgo la seguridad de la información.

CONCLUSIÓN

Con esto aprendimos la importancia del testing en las áreas de trabajo, el resguardo que hay que tener de los sistemas para no faltar a las políticas de seguridad, la importancia de documentar los sucesos para tener referencia y registros de las anomalías para poder producir un buen plan de mitigación, con el cuál podamos prevenir todo tipo de incidente.

GRACIAS

Bastian Fierro – Daniel Santibañez – Tamar Andrade

contacto@ghostcode.com

www.ghostcode.com