VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Hacker Mate

Descifrando la kriptonita de la capa 8

Hacker Mate

Descifrando la kriptonita de la capa 8

- La Kriptonita - El Atacante.
- La Capa 8 - El Superusuario.
- Ajedrez de la ciberdefensa.
- El Descenlace: Kriptonita Vs Superusuario

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Expositor: Ing. Eliezer Montaño

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

La Kriptonita

El Atacante

De: **Amazon.com** <custumerservices@amazon.com>
Date: 27 oct 2023 a la(s) 14:00
Subject: Tu App de Amazon necesita ser actualizada de inmediato
To: superusuar/o@gmail.com

amazon

Tu App de Amazon necesita ser actualizada de inmediato

Protege tus datos crediticios

Debido a actualizaciones en nuestras plataformas, no ha sido posible actualizar su APP de manera automática.

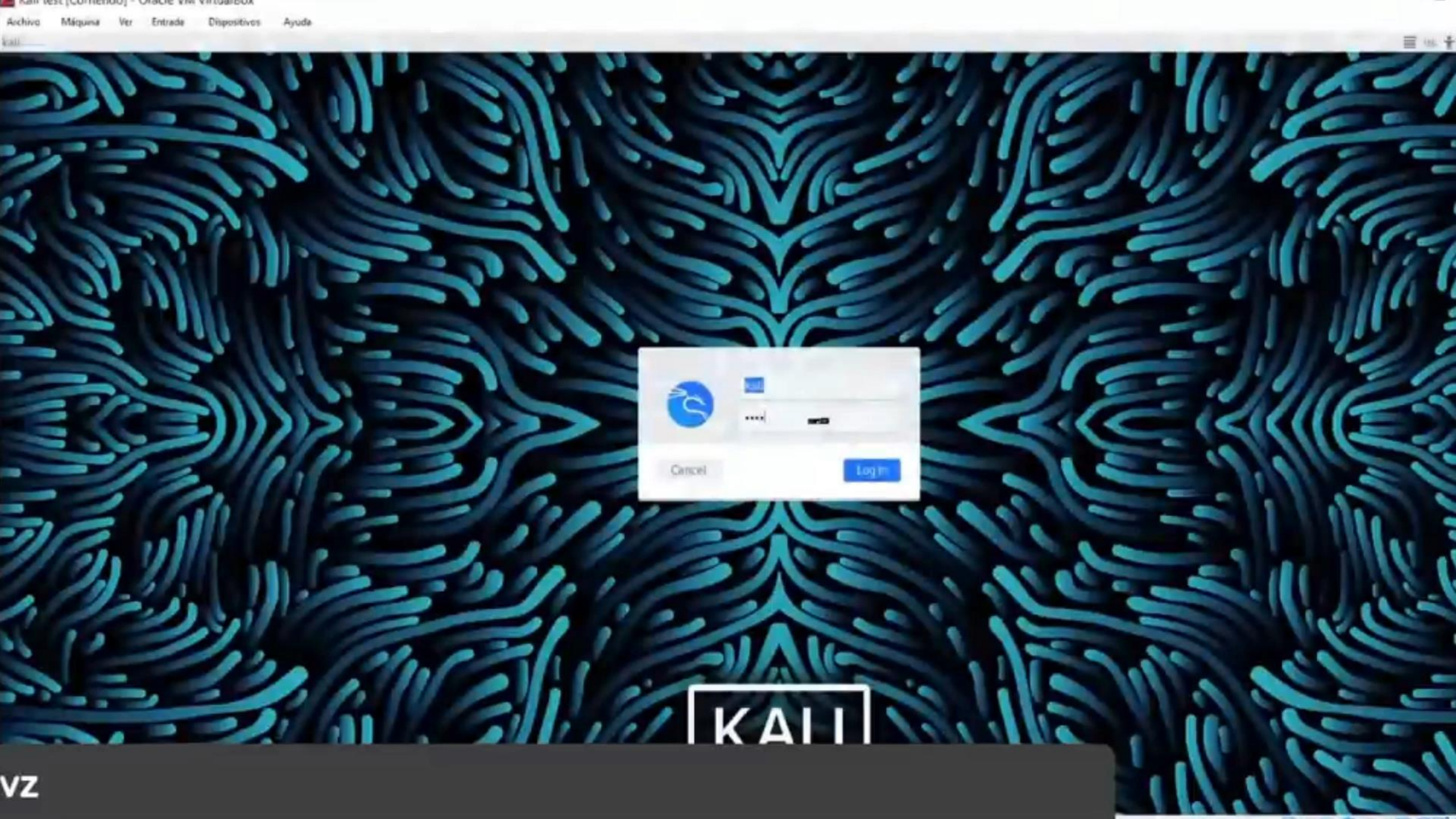
Si no actualizada su APP en las próximas 24 horas, su cuenta de Amazon quedará desactivada permanentemente. Para continuar usando su cuenta, por favor **visite este link** para descargar la nueva versión oficial de nuestro APP y así poder garantizar la protección de sus datos.

Gracias.

Servicio al Cliente Amazon.com

Kriptonita Pura

La Estrategia Maligna


Archivo
Máquina
Ver
Entrada
Dispositivos
Ayuda
Cancel
Log In
KALI

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

La Capa 8

El Superusuario

Capa 8

La capa 8 es atacada

De: **Amazon.com** <custumerservices@amazon.com>
Date: 27 oct 2023 a la(s) 14:00
Subject: Tu App de Amazon necesita ser actualizada de inmediato
To: superusuario@gmail.com

amazon

Tu App de Amazon necesita ser actualizada de inmediato

Protege tus datos crediticios

Debido a actualizaciones en nuestras plataformas, no ha sido posible actualizar su APP de manera automática.

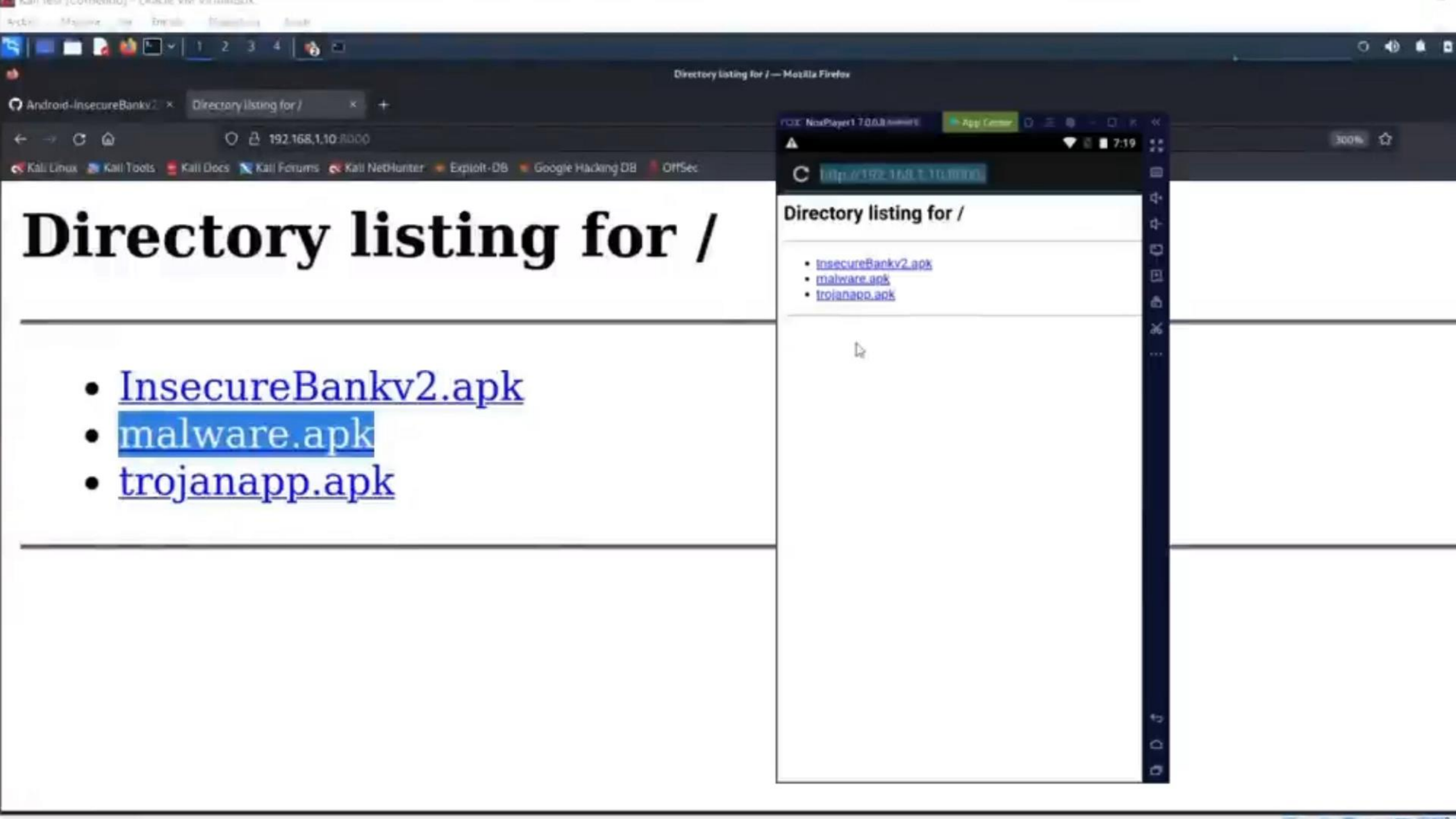
Si no actualizada su APP en las próximas 24 horas, su cuenta de Amazon quedará desactivada permanentemente. Para continuar usando su cuenta, por favor **visite este link** para descargar la nueva versión oficial de nuestro APP y así poder garantizar la protección de sus datos.

Gracias.

Servicio al Cliente Amazon.com

Se mueve el ajedrez

Caer en la Trampa


Directory listing for / — Mozilla Firefox
Android-InsecureBankv2
Directory listing for /
192.168.1.10:8000
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Directory listing for /
InsecureBankv2.apk
malware.apk
trojanapp.apk
7:19
Directory listing for /
InsecureBankv2.apk
malware.apk
trojanapp.apk

KRITONITA

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

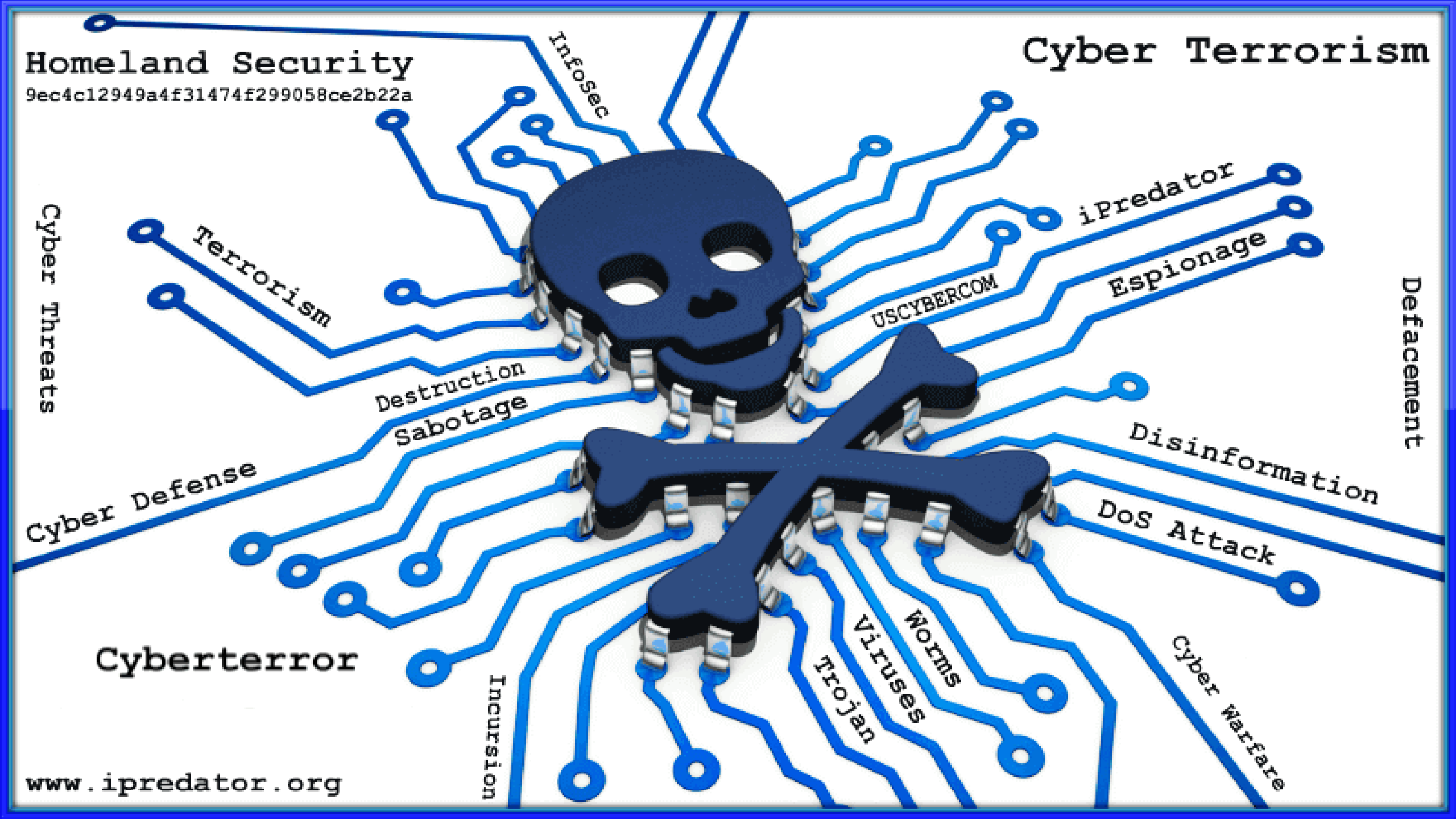
El Ajedrez

De la Ciberdefensa

El Ajedrez

El Tablero de Juego

Conociendo el Terreno de Batalla


Homeland Security
9ec4c12949a4f31474f299058ce2b22a
Cyber Terrorism
Infosec
Cyber Threats
Terrorism
iPredator
Espionage
USCYBERCOM
Defacement
Destruction
Sabotage
Disinformation
Cyber Defense
DoS Attack
Cyberterror
Incursion
Trojan
Viruses
Worms
Cyber Warfare
www.ipredator.org

Estrategia de ciberdefensa – Ayudar a ganar a Superusuario

Apoyar a Superusuario para que esta vez gane esta partida. Juntos podremos lograr que la empresa Superusuario sea más segura

Apoyando en la estrategia de toma de decisicones relacionadas a la Ciberseguridad

Si ganamos esta partida habrá tres finalistas, a quienes Superusuario entregará 3 premios.

En el siguiente slide podrás escanear un código QR que te permitirá participar.

Escanea para participar

- Kriptonita Vs Superusuario

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

El Desenlace

Kriptonita Vs Superusuario

En la otra esquina…
El atacante **Kriptonita**

En esta esquina…
La Empresa **Superusuario**

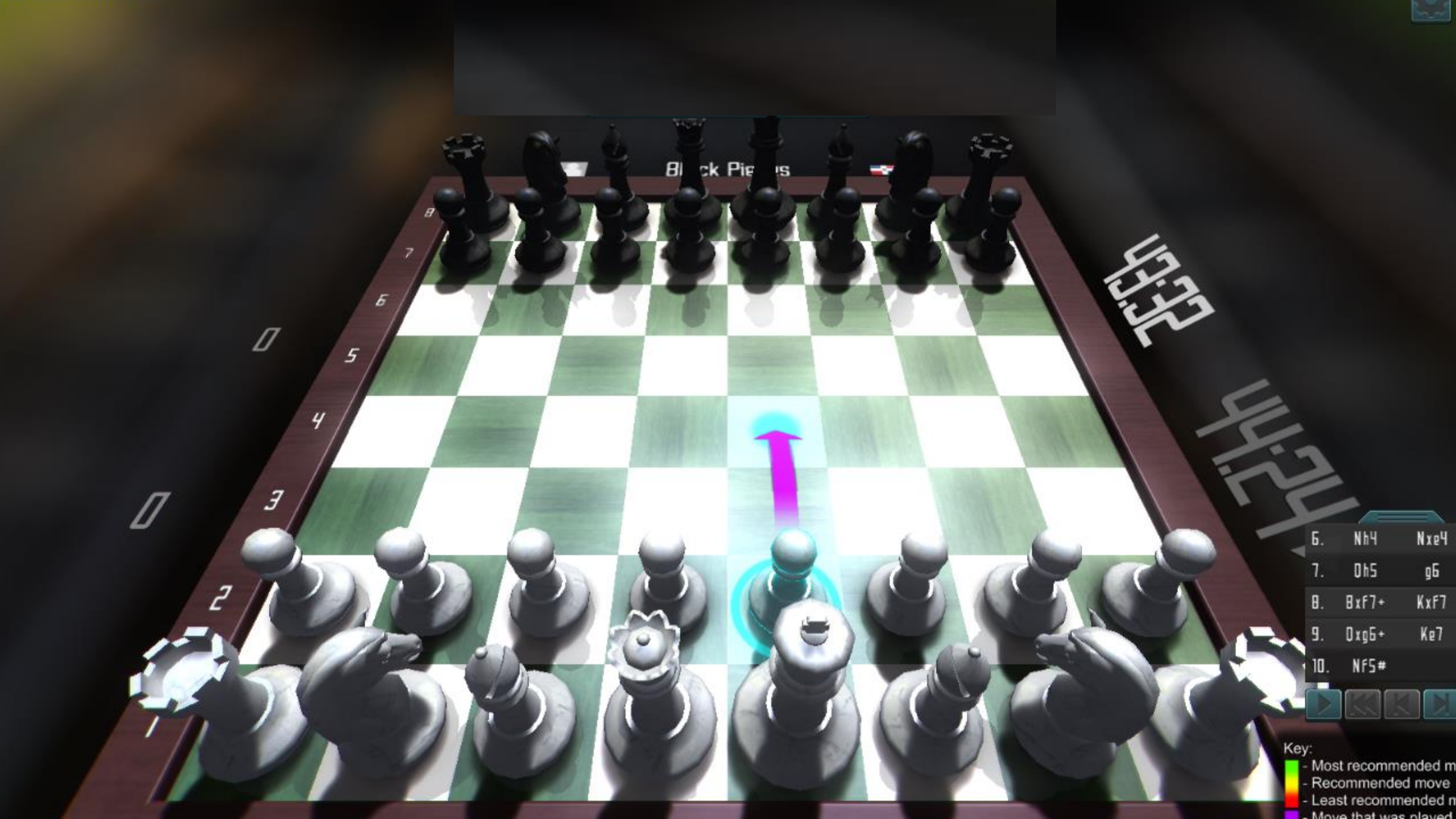

Resign
Draw
15:00
0
0

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Superusuario

Empresa SUPERUSUARIO lanza sus operaciones al mercado ofreciendo servicios de asesoría financiera a grandes y medianas empresas. Instala sus oficinas centrales en una de las principales torres comerciales del Distrito Nacional en RD. Contando con una red de otras sucursales en diferentes partes de Santo Domingo.

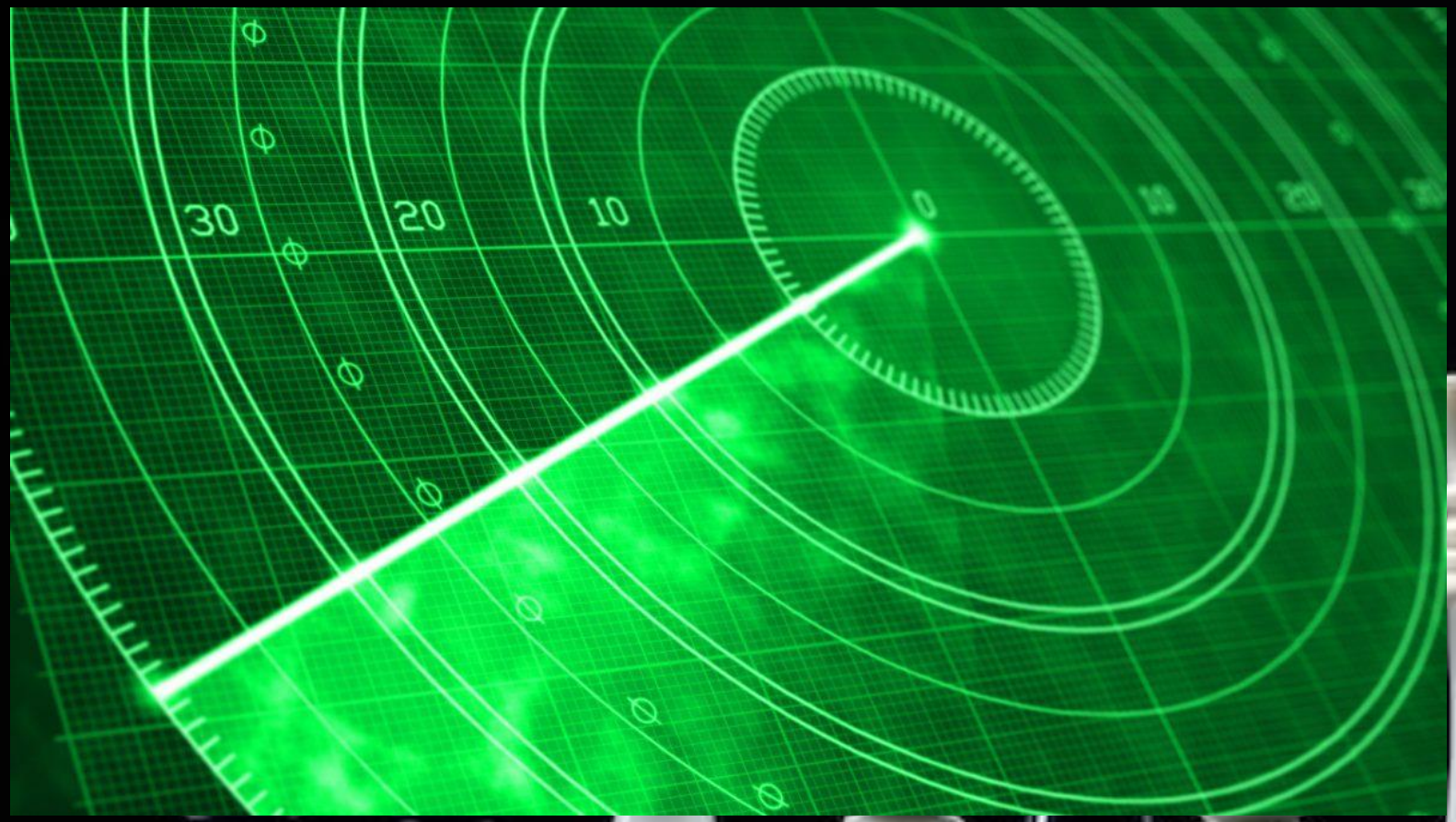
Jugada 1


6. Nh4 Nxe4
7. Oh5 g6
8. BxF7+ KxF7
9. Oxg6+ Ke7
10. NF5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Kriptonita

Atacante Kriptonita es contratado para robar secretos empresariales de la empresa SUPERUSUARIO. A través de un escaneo de puertos, examina las defensas de la víctima para saber a qué se enfrenta.



Jugada 1


6. Nh4 Nxe4
7. Qh5 g6
8. BxF7+ KxF7
9. Qxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Superusuario

Tomar una decisión estratégica frente al ataque anterior.

¿Qué medidas implementarías para detener este ataque?

Implementar Pivilege Access Manager para administrar las credenciales con altos privilegios.

Implementar Firewall, IPS

Endurecer las políticas de password.

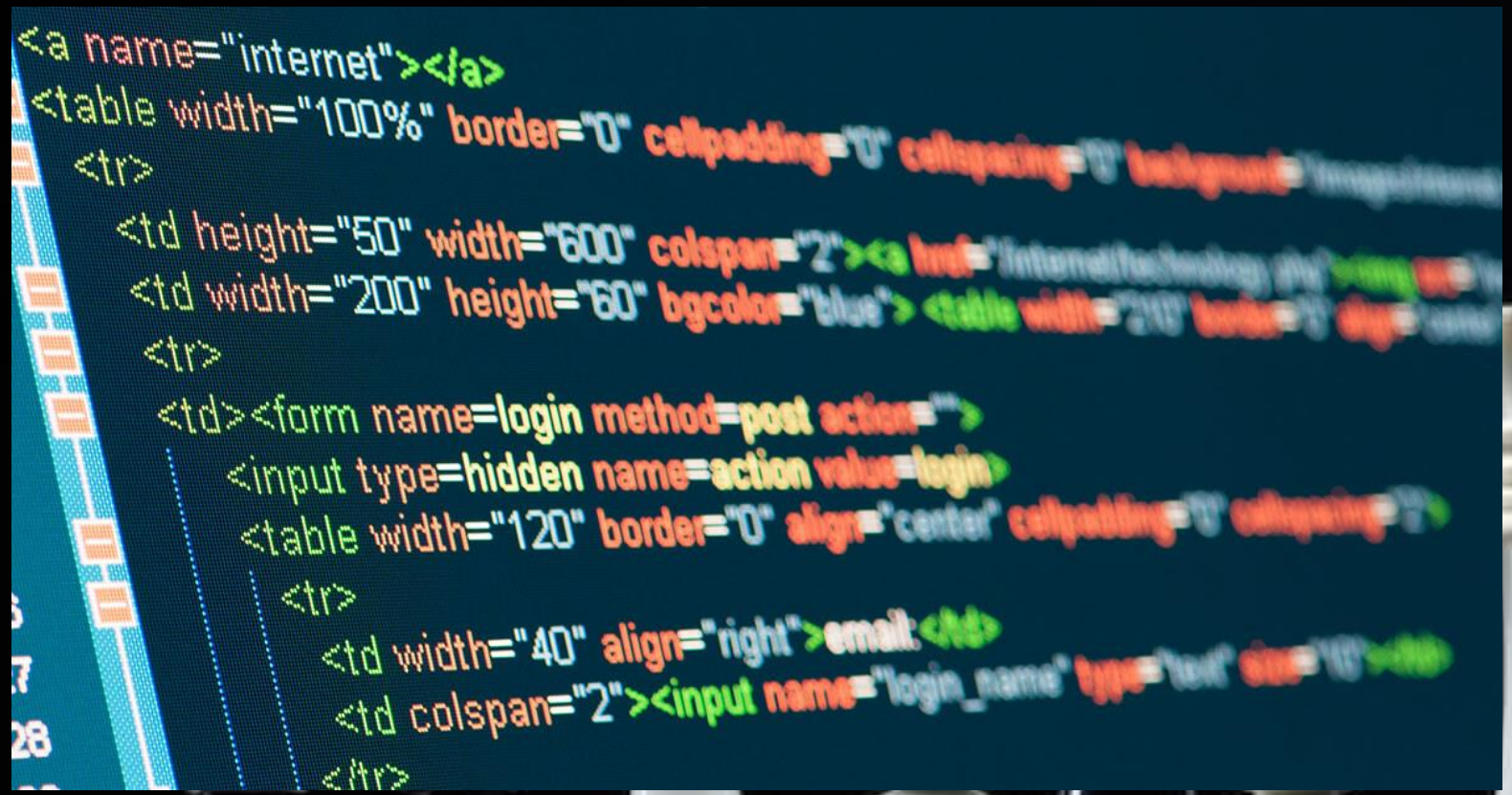
Hacer cumplir el principio de privilegios mínimos para reducir la superficie de ataque y controlar la elevación


Black Pieces
8
7
6
5
4
3
2
1
6. Nh4 Nxe4
7. Oh5 g6
8. BxF7+ KxF7
9. Oxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

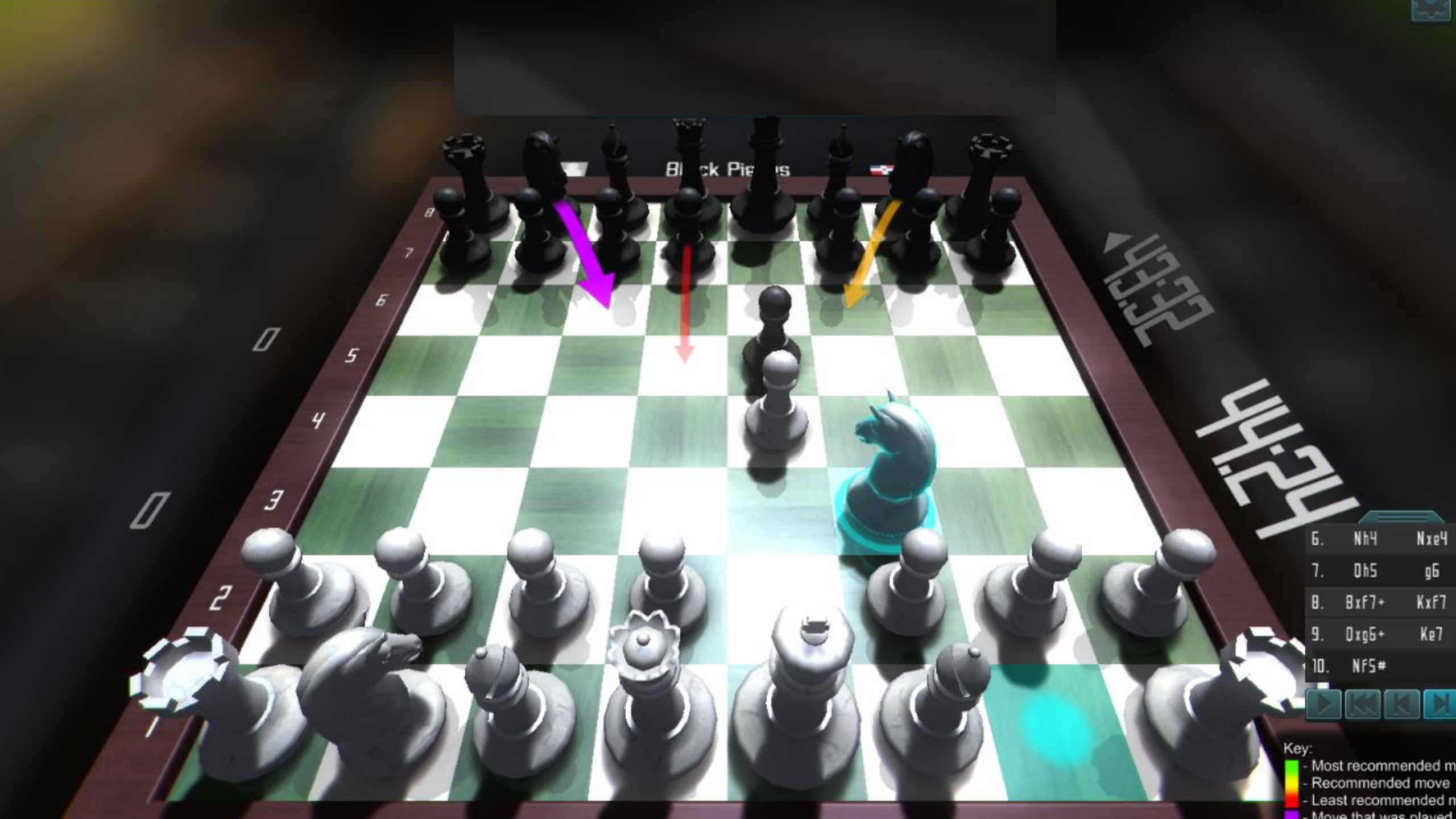
VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Kriptonita

Atacante: Roba las credenciales de la página web de una de los suplidores de la empresa. Este suplidor no es muy conocido y no le presta atención a su seguridad. El sitio web del suplidor es muy frecuentado por los empleados de la empresa. El atacante, ya con el control de esta página, procede a colocar una trampa que instala un malware tan pronto se navega en el sitio.



Jugada 2


6. Nh4 Nxe4
7. Qh5 g6
8. BxF7+ KxF7
9. Qxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

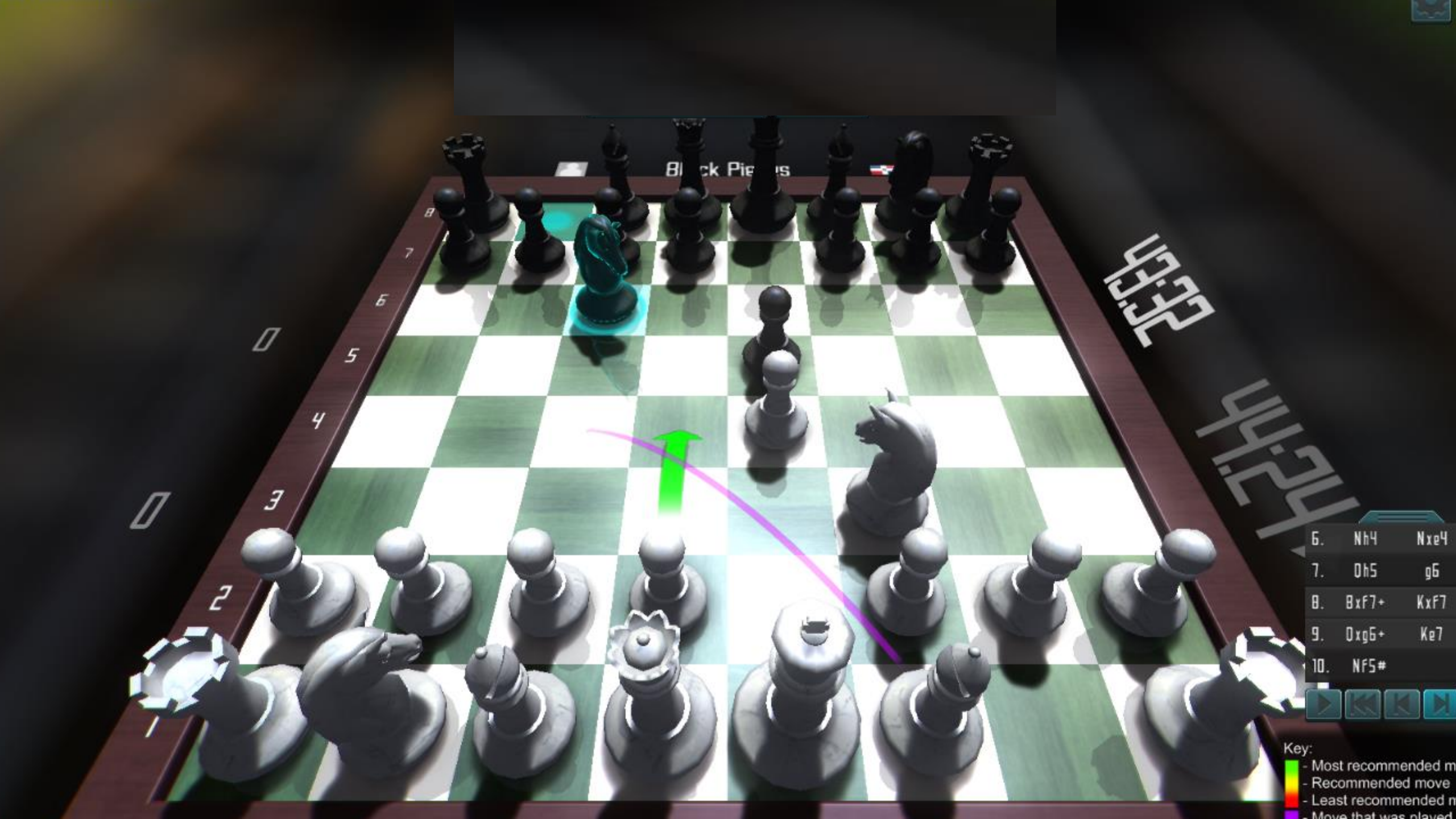
VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Superusuario

Tomar una decisión estratégica frente al ataque anterior.

Software de seguridad de la empresa SUPERUSUARIO, reconoce el URL malicioso que alojaba el kit de exploits y la dirección e IP fueron bloqueados automáticamente. ¿Qué medidas puede implementar el suplidor para disminuir las posibilidades de que su sitio web vuelva a ser comprometido? Escoge las que apliquen:

- Limitar el número de autenticaciones que suceden desde una misma dirección IP o desde un mismo usuario
- Implementar el protocolo WPA3, el cual soporta el Perfect Forward Secrecy.
- Implementar un Web Application Firewall
- Utilizar captcha y múltiple factor de autenticación
- Utilizar una VPN.

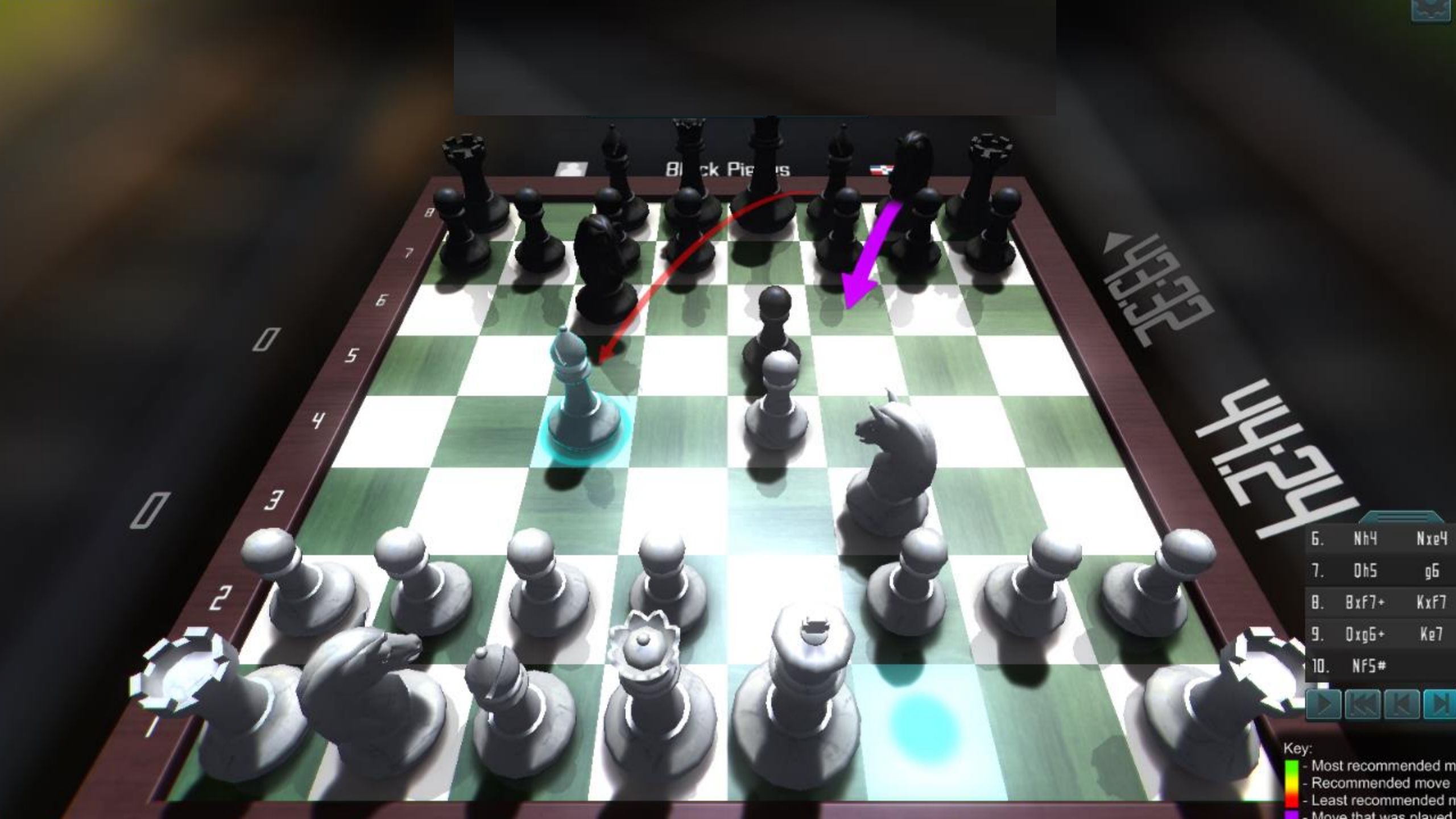

6. Nh4 Nxe4
7. Oh5 g6
8. BxF7+ KxF7
9. Oxg6+ Ke7
10. NF5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Kriptonita

Atacante prepara el ataque con el Truco de la memoria flash gratis. Utilizando una Memoria Usb Rubber Ducky, procede a programar un ataque para tomar control remoto de la víctima, con solo conectar la memoria USB. El atacante deja caer la memoria cerca de la entrada de la empresa. Empleada la recoge y la lleva dentro de la oficina con el objetivo de verificar lo que tiene dentro y poder devolverla a su dueño

Jugada 3


6. Nh4 Nxe4
7. Qh5 g6
8. BxF7+ KxF7
9. Qxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

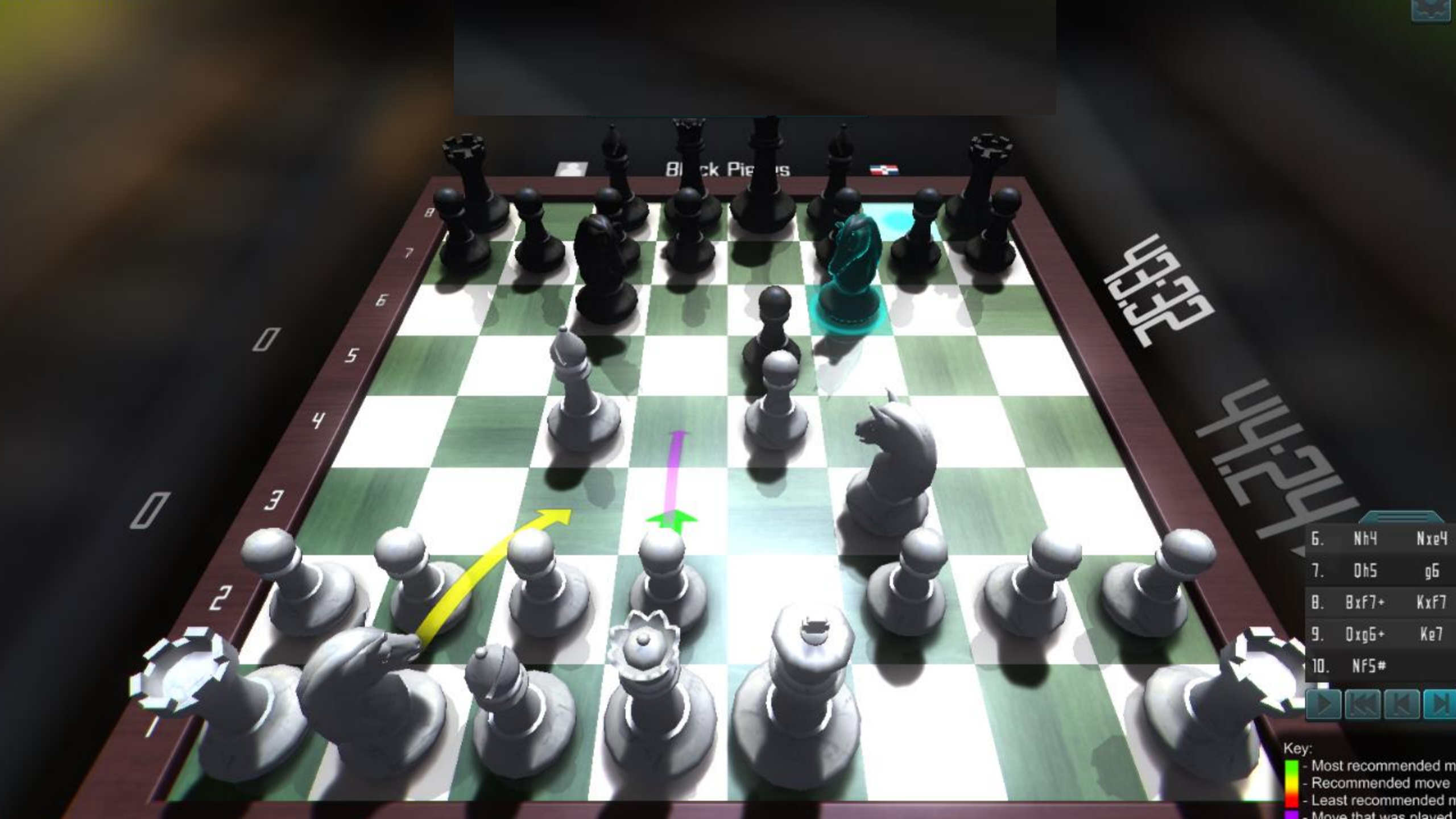
Juega Superusuario

Tomar una decisión estratégica frente al ataque anterior.

Cuáles de las siguientes medidas aplicarías con el fin de evitar el ataque del Rubber Ducky?

Escoge todas las que apliquen:

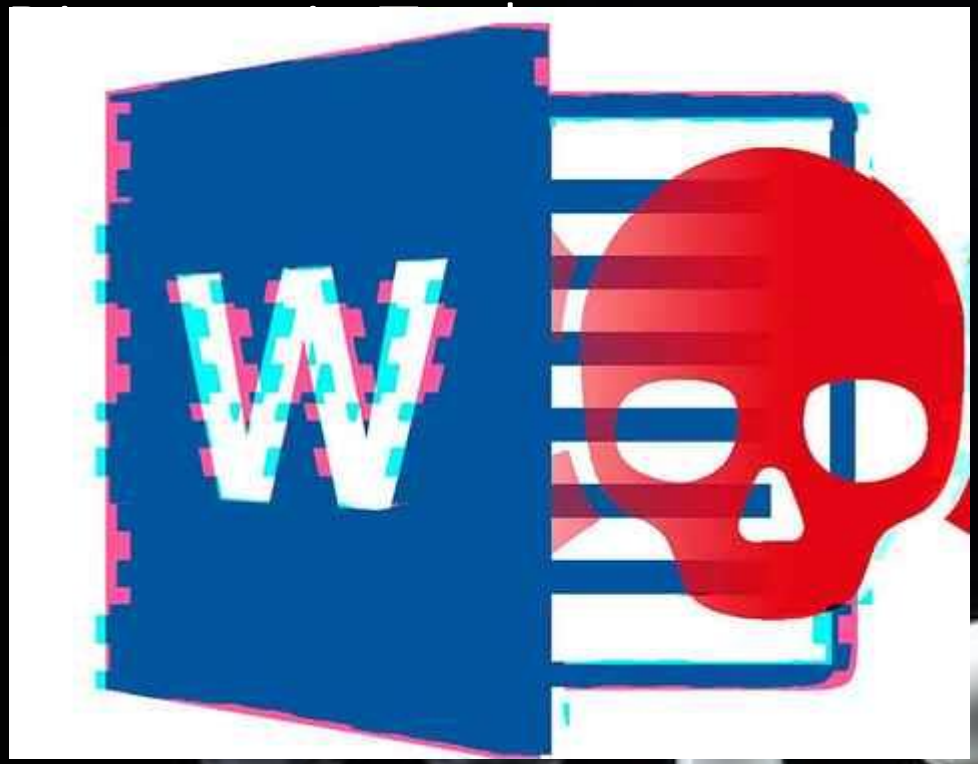
- Sin excepción, bloquear los puertos USB para todo tipo de dispositivo, ya que el Rubber Ducky es detectado como un teclado.
- Limitar el uso de CMD y Powershelll sin introducir la contraseña de usuario.
- Uso de Duckhunter para monitorear el uso del teclado para ver la velocidad con la que se escribe y detectar en qué aplicación se está escribiendo
- Uso de un dispositivo tipo llave llamado USB Port Blocker
- Mediante El Registro de Windows, modificar la columna Datos de la sección Start, dentro de HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor


6. Nh4 Nxe4
7. Oh5 g6
8. BxF7+ KxF7
9. Oxg6+ Ke7
10. NF5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Kriptonita

El atacante diseña un correo electrónico falso y lo envía el Viernes 4:30 pm, a nombre del personal de Gestión Humana. Es un correo muy llamativo, con lista del personal calificable para aumento en el mes siguiente. Lleva adjunto un documento de texto Word con el código malicioso previamente integrado, el cual aprovecha una vulnerabilidad que tiene la herramienta Microsoft Support

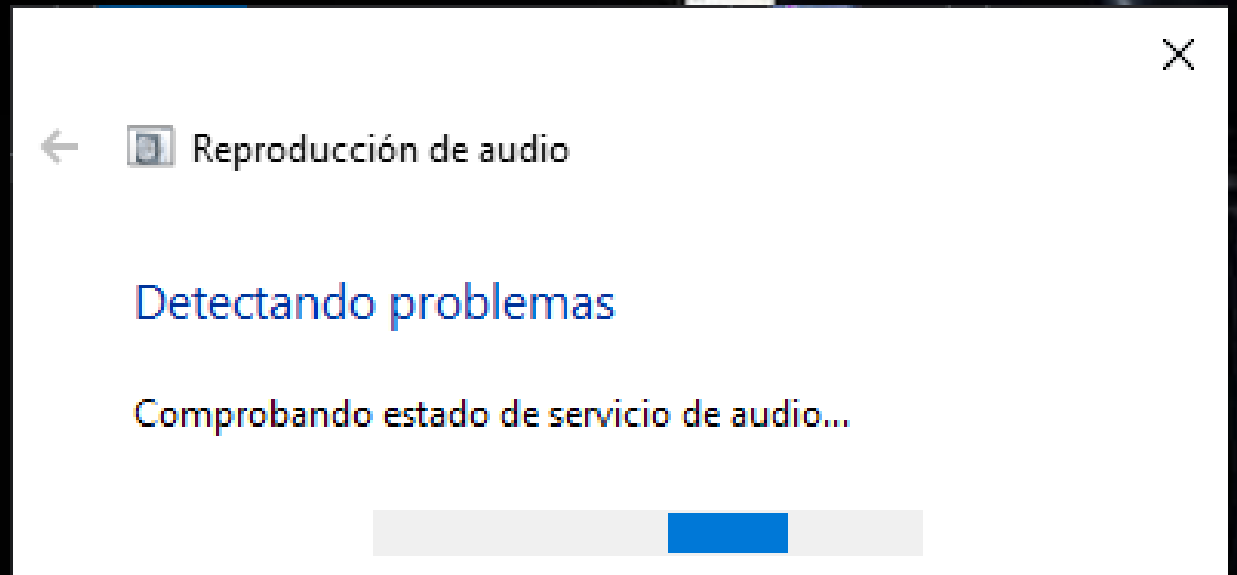


Jugada 4

Un usuario de negocios desesperado por un aumento, abre el correo y con solo abrir el documento de Word, se ejecuta la herramienta de diagnóstico de soporte de Microsoft y le permite la ejecución del código remoto, permitiendo el paso a los atacantes.

Jugada 4

La vulnerabilidad de Microsoft Office y Windows llamada Follina (CVE-2022-30190) es la responsable de este tipo de ataques. El Atacante descubre que en la empresa existen equipos con sistemas operativos desactualizados, esto debido a que hay un aplicativo de negocio legacy que no permite aplicar actualizaciones. Esto le permitió al atacante diseñar un ataque que se aprovecha de esta falla que permite la ejecución remota de comandos sin necesidad de hacer un solo clic. Esta falla de seguridad está relacionada con la herramienta MSDT.



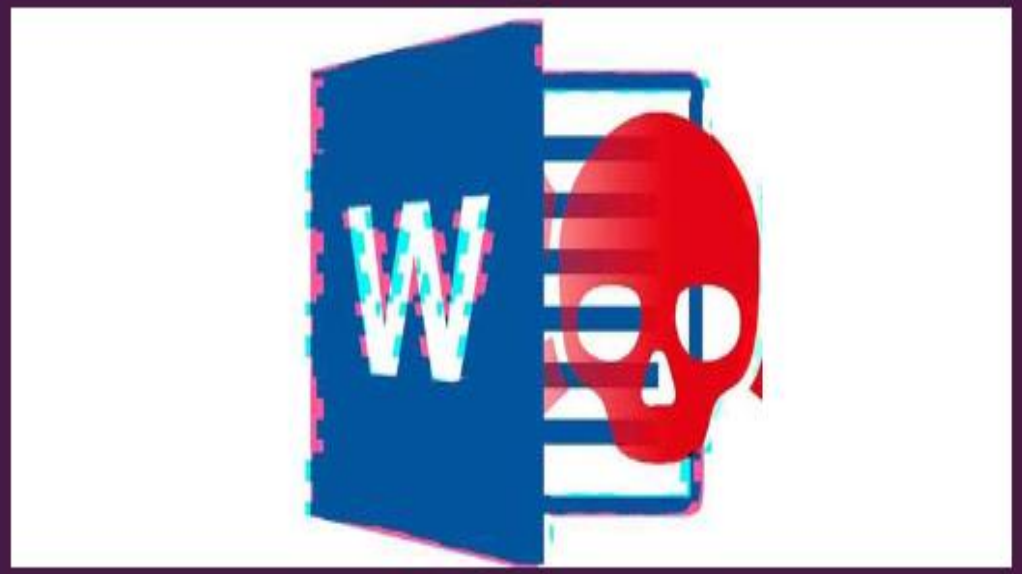
Jugada 4


6. Nh4 Nxe4
7. Oh5 g6
8. BxF7+ KxF7
9. Oxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

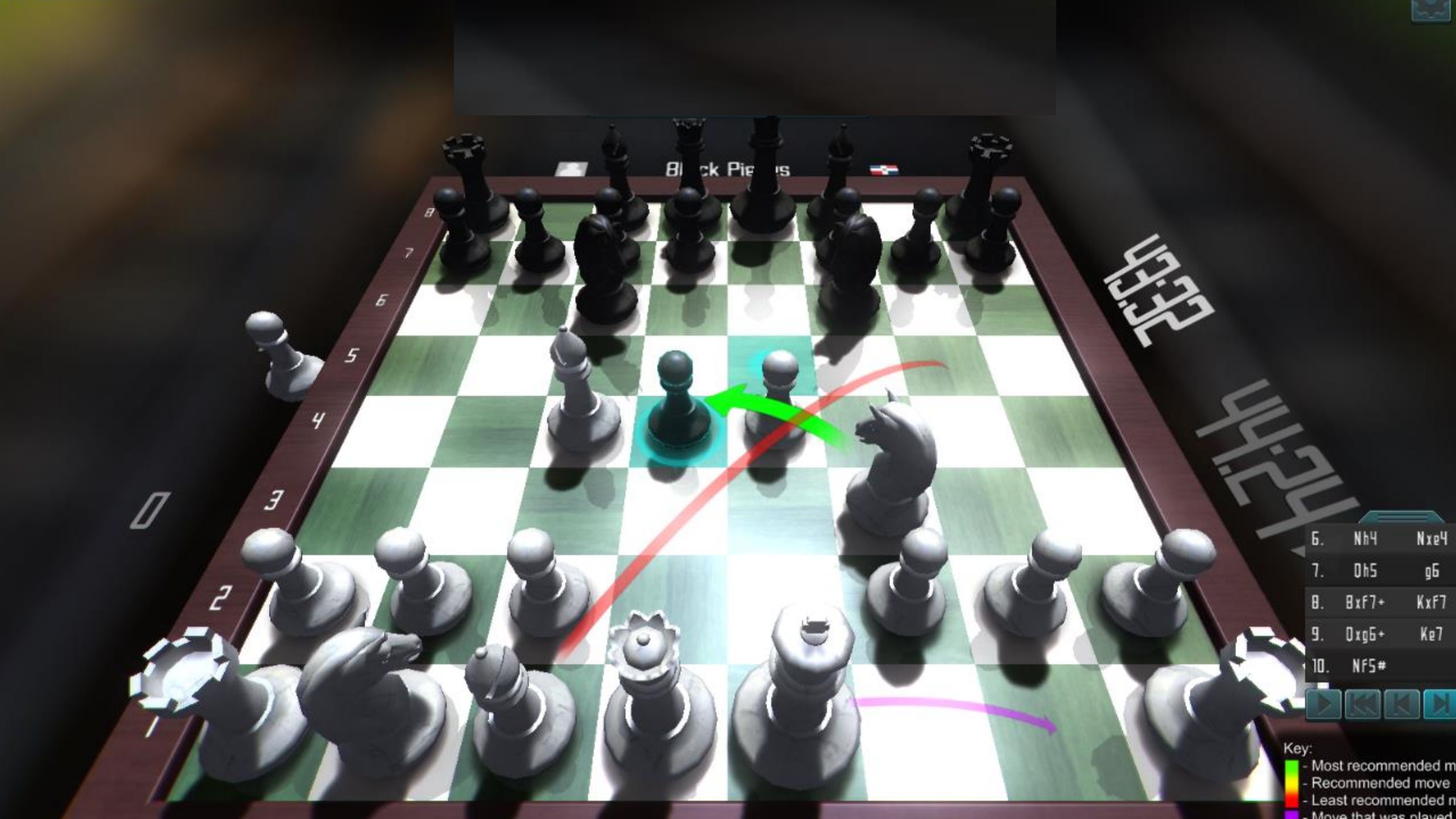
Juega Superusuario

Tomar una decisión estratégica frente al ataque anterior.



¿Cuáles acciones impulsarías en la empresa para evitar que ocurra este tipo de ataque? Escoja las que apliquen::

- APrevenir el robo de cookies.
- Realizar ejercicios de phishing Ético.
- Fortalecer programa de CONCIENTIZACIÓN CIBERSEGURIDAD
- Detectar y bloquear amenazas que intentan acceder a los repositorios de credenciales en los endpoints.
- Deshabilitar el Protocolo MSDT URL


6. Nh4 Nxe4
7. Oh5 g6
8. BxF7+ KxF7
9. Oxg6+ Ke7
10. NF5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Kriptonita

Atacantes han roto las defensas combinando un exploit de día cero con la ingeniería social para que la víctima abra el código malicioso. Ahora esa PC está bajo su control y pueden utilizar esa cuenta de usuario para comenzar a explotar la red sin que sean detectados.

Jugada 5

Realizan ataque de robo de credenciales mediante el volcado del contenido de todos los repositorios claves de los sistemas.

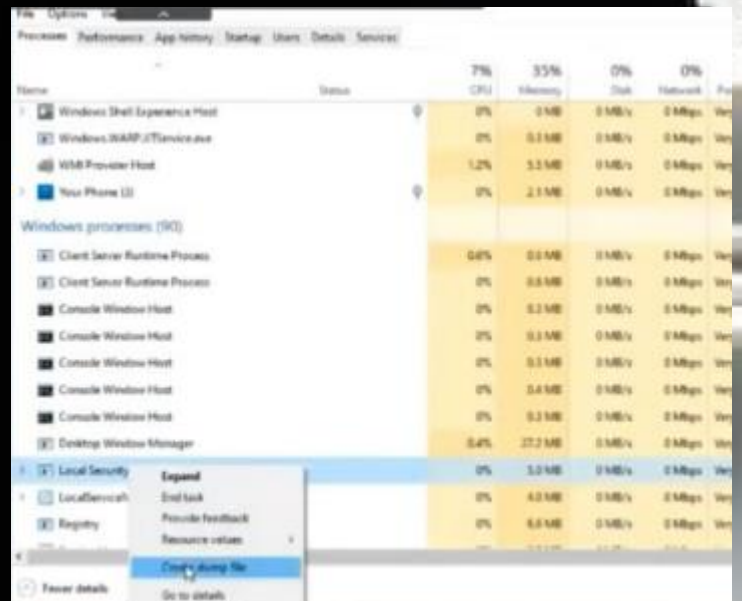
Jugada 5


6. Nh4 Nxe4
7. Oh5 g6
8. BxF7+ KxF7
9. Oxg6+ Ke7
10. NF5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

El robo de credenciales involucra: LSAS, navegadores, Github, AWS, Pipilines de desarrollo, aplicaciones, procesos del sistema, ubicaciones del Registro, rutas de archivos conocidas.

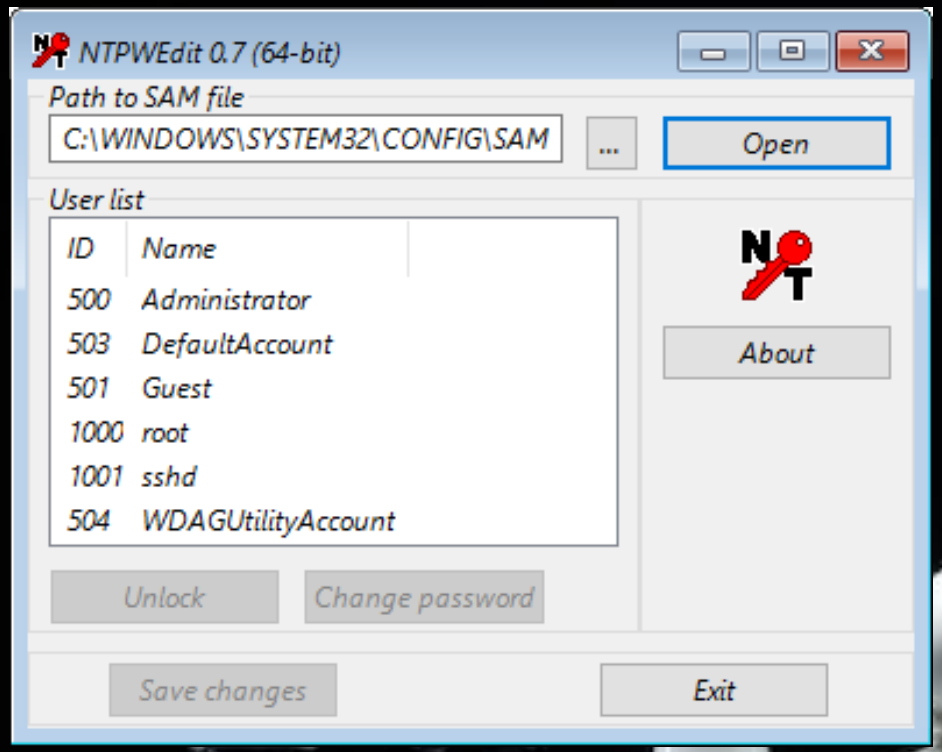
Jugada 5

LSASS memory: Contraseñas de texto no cifrado de sesiones iniciadas, vales Kerberos, claves de cifrado Kerberos, códigos PIN De SmartCard/Token, hashes LM/NTLM, clave de copia de seguridad de dominio DPAPI, información de autenticación de confianza de dominio, MasterKeys DPAPI almacenadas en caché, SysKey almacenada en caché (necesidad de descifrar secretos sam/LSA/credenciales almacenadas en caché/NTDS,clit), contraseñas de texto claro de cuentas, almacenadas en el Administrador de credenciales.



Jugada 5

SAM: El Administrador de cuentas de seguridad. Este es un archivo de base de datos en los sistemas operativos Microsoft Windows que almacena las contraseñas de los usuarios. Se puede utilizar para autenticar usuarios locales y remotos. SAM utiliza medidas criptográficas para evitar que los usuarios prohibidos obtengan acceso al sistema.



Jugada 5

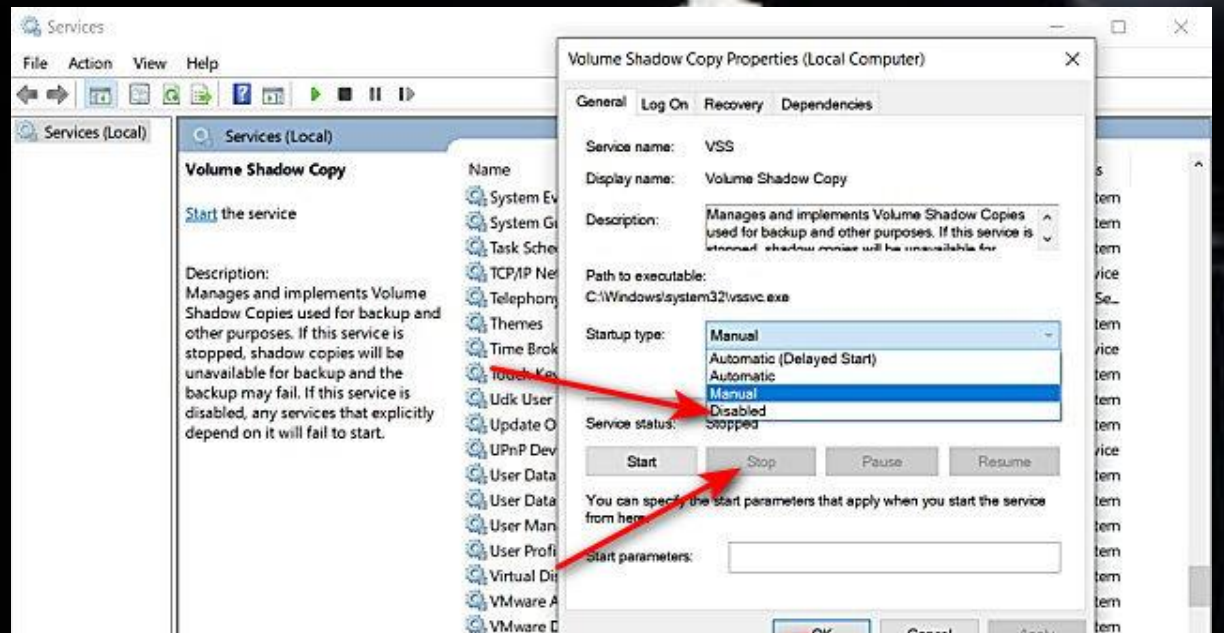
NTDS.dit file: Hashes de cuentas de dominio, clave de copia de seguridad de dominio. Se encuentra en:

C:\Windows > Program Files (x86) > Common Files >

Jugada 5

Shadow Copy (VSS): Son cuentas que se utilizan para autenticaciones con cierto nivel de privilegios. Tambien se pueden encontrar en los archivos SAM/SECURITY/NTDS.dit.

Las aplicaciones también pueden tener un almacén copias de credenciales interno que se puede abusar. Por ejemplo, Filezilla exporta todas las credenciales almacenadas a un archivo XML local. Como la ruta de acceso es la misma en todas las instalaciones, los atacantes pueden buscar estas ubicaciones conocidas.



Jugada 5

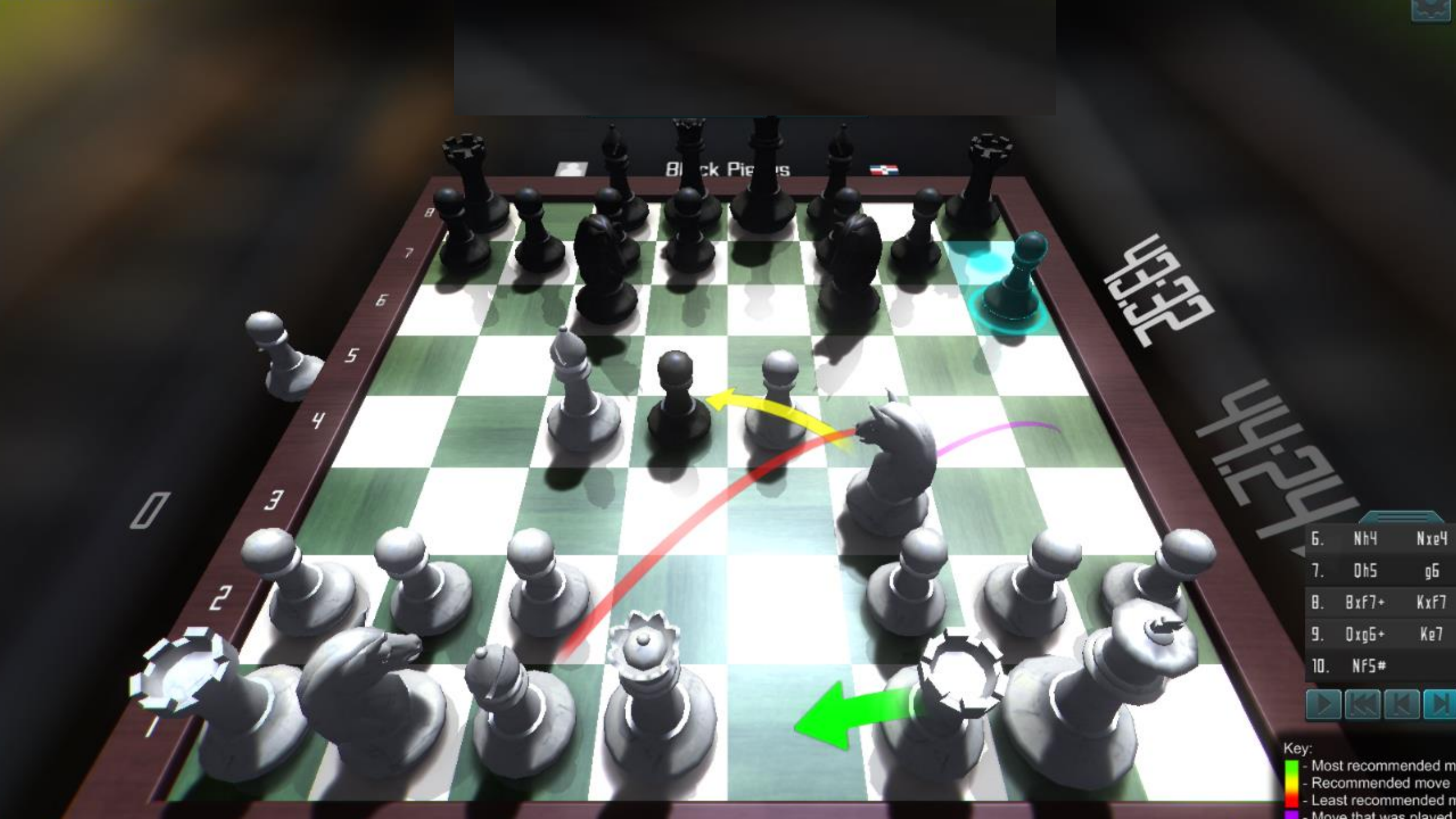
VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Superusuario

Tomar una decisión estratégica frente al ataque anterior.

¿Cuáles acciones impulsarías en la empresa para mitigar la ocurrencia del ataque del robo de credenciales? Escoja las que apliquen:

- Detectar y bloquear amenazas que intentan acceder a los repositorios de credenciales en los endpoints.
- implementar un sistema de detección y prevención de intrusiones (IDS/IPS)
- Utilizar aislamiento de sesiones para prevenir el residuo de credenciales en los equipos.
- Eliminar credenciales quemadas en las aplicaciones, scripts y repositorios de código
- Colocar un Firewall


6. Nh4 Nxe4
7. Qh5 g6
8. BxF7+ KxF7
9. Qxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Kriptonita

Atacante: Busca moverse lateralmente en la red. Encuentra un correo electrónico de otro usuario con acceso a las BD importantes de la empresa. Dicho usuario se convierte en el nuevo blanco de ataque. Procede a vaciar el caché local de contraseñas, obteniendo las credenciales del administrador local, pero aún no del administrador de dominio que es su objetivo.

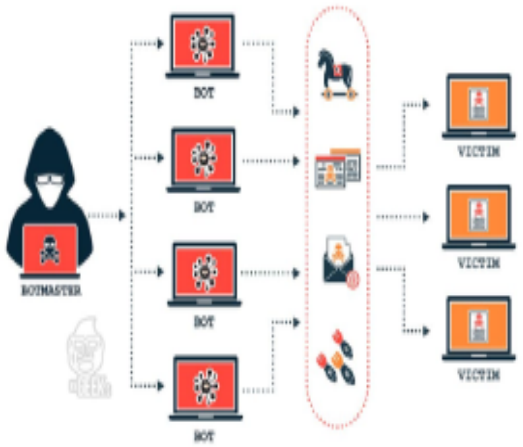
Jugada 6


6. Nh4 Nxe4
7. Qh5 g6
8. BxF7+ KxF7
9. Qxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Superusuario

Tomar una decisión estratégica frente al ataque anterior.



¿Qué acciones tomarías para prevenir el movimiento lateral en la red?

Implementar el protocolo WPA3, el cual soporta el Perfect Forward Secrecy

Utilizar aislamiento de sesiones para prevenir el residuo de credenciales en los equipos

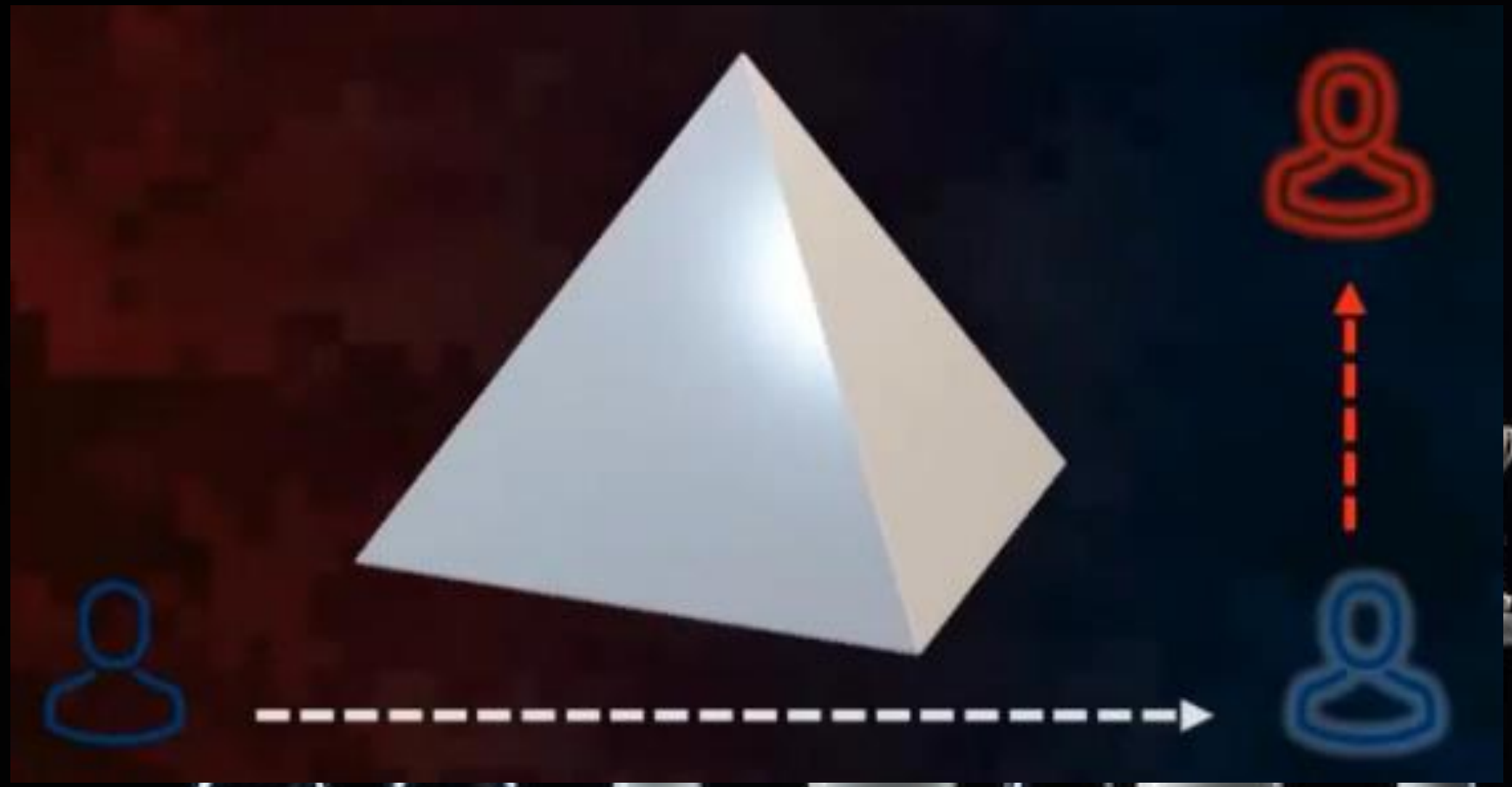
Hacer cumplir el acceso Just In Time (JIT) para minimizar los privilegios permanentes.

Aleatorizar credenciales para eliminar la reutilización de cuentas y reducir el tiempo de vida.

Implementar un Web Application Firewall.

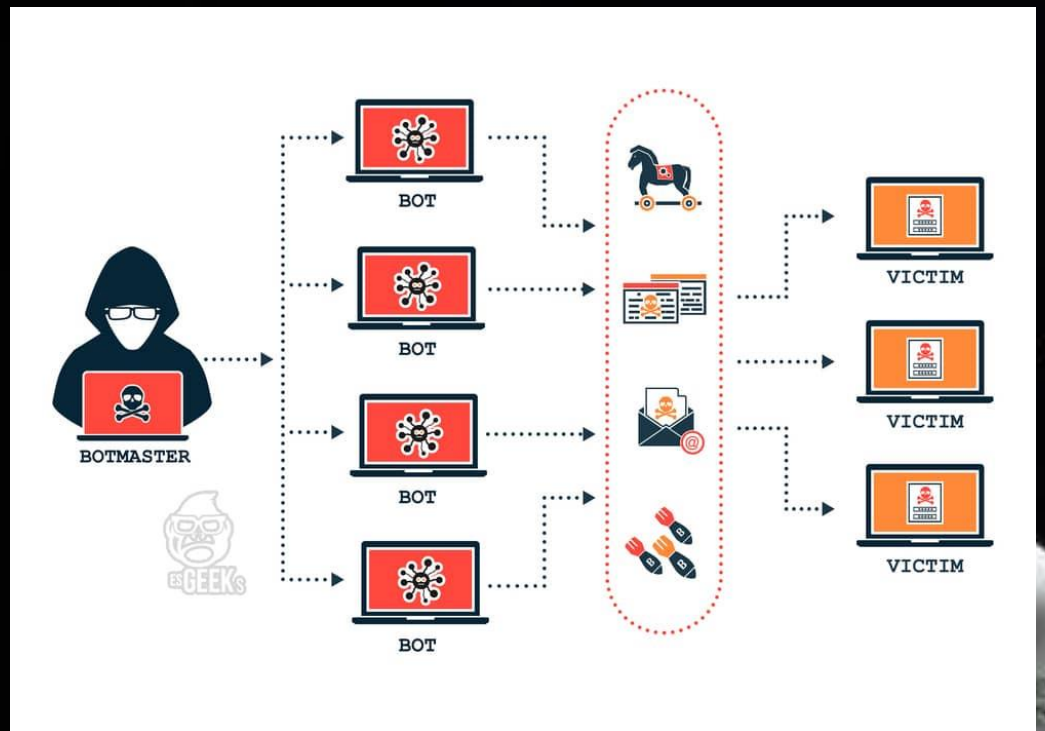

6. Nh4 Nxe4
7. Oh5 g6
8. BxF7+ KxF7
9. Oxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

Atacante realiza movimiento lateral, utilizando técnicas para moverse progresivamente a través de la red, buscando datos y activos clave específicos.



Jugada 6

En el movimiento lateral son utilizadas las herramientas y características de TI legítimas integradas en el sistema operativo, permitiéndole a los atacantes moverse fácilmente por la red, recopilar la información necesaria y transferir datos sin activar ninguna alarma de las defensas de seguridad.



Jugada 6

Herramientas que incluyen SMB, Ping, Perl, Windows Credential Editor, Telnet, FTP, SSH, PSTools, RDP, CMD, Powershell y WMI. Utilizando la tecnica del abuso de las cuentas SPN (Kerberoasting). Estas son cuentas de servicios con privilegios, para escalar privilegios con un usuario valido del sistema y generar sus propios tickets de autenticación más adelantes.

Jugada 6

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Kriptonita

Atacantes instalan malware keylogger en uno de los equipos de la red, con el objetivo de capturar información sobre el usuario y la empresa.

Jugada 7


6. Nh4 Nxe4
7. Qh5 g6
8. BxF7+ KxF7
9. Qxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Superusuario

Tomar una decisión estratégica frente al ataque anterior.

Anti Malware detecta y elimina un BOT en una de las PC de la empresa y lo califica como una brecha menor.

¿Qué acción realizarías de manera inicial ante tal detección de este malware?

- Copiar todo el contenido del disco duro y pegarlo en un disco duro portatil
- Aislar la PC, hacer una copia de la RAM y luego una copia forense del disco.
- Llamar al usuario para que desconecte inmediatamente la alimentación eléctrica de la PC.
- Recuperar el archivo malicioso y subirlo a la plataforma VirusTotal.
- Apagar la PC y tomar una copia forense del disco.


6. Nh4 Nxe4
7. Qh5 g6
8. Bxf7+ Kxf7
9. Qxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Kriptonita

Atacante busca previamente utilizar técnicas anti-forense, ofuscando el código fuente del malware, codificándolo en base64.

Jugada 8


6. Nh4 Nxe4
7. Oh5 g6
8. BxF7+ KxF7
9. Oxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Superusuario

Tomar una decisión estratégica frente al ataque anterior.

¿Cuál de las siguientes herramientas utilizarías para procesar la evidencia digital recabada y dar una respuesta a este incidente? Tomando en cuenta que necesitas una herramienta capaz de procesar la evidencia digital, conseguir el archivo malicioso ejecutable a los fines de realizar ingeniería reversa y decodificar el base64.

- Cellebrite
- FTK Imager
- Volatility
- Magnet Axiom
- Clonador forense Tableau TD2u


Black Pieces
6. Nh4 Nxe4
7. Oh5 g6
8. BxF7+ KxF7
9. Oxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Kriptonita

Atacante realiza ataque de Golden Ticket, realizando una escalada y abuso de privilegios de la cuenta de comprometida previamente.

Jugada 9

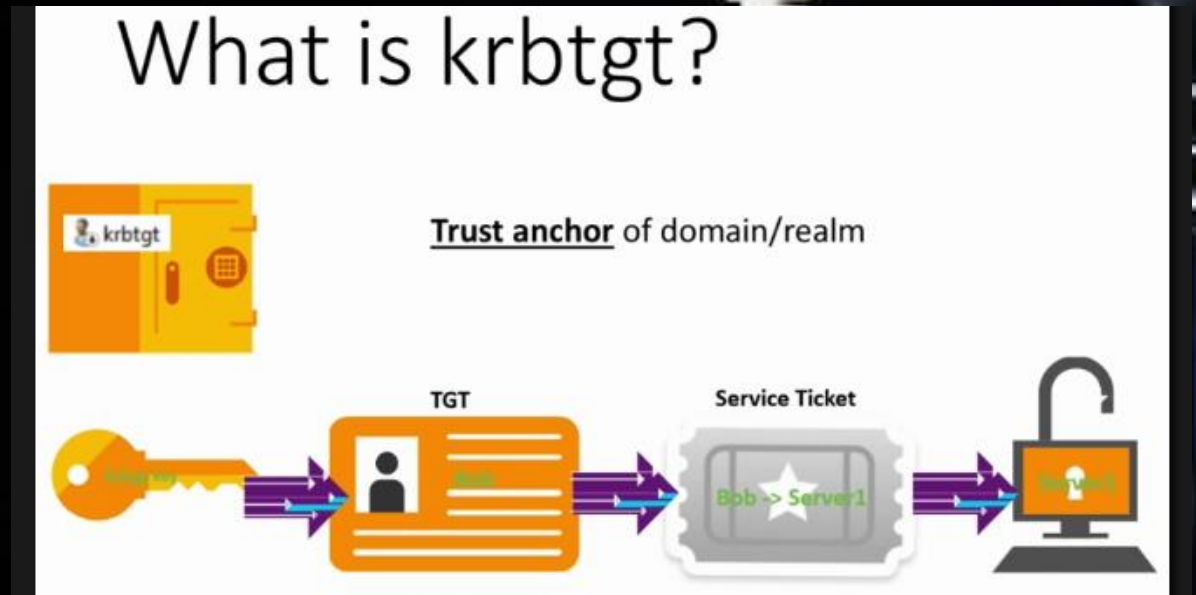
Mediante un ataque de fuerza bruta contra el servidor de la base de datos les da acceso de ROOT (admin) teniendo el permiso para copiar todo el código fuente de un proyecto crítico en el que está trabajando la empresa SUPERUSUARIO. Intenta copiar el botín fuera de la red, hasta sus servidores en la deep web.

Jugada 9


Black Pieces
6. Nh4 Nxe4
7. Qh5 g6
8. BxF7+ KxF7
9. Qxg6+ Ke7
10. Nf5#
Key:
- Most recommended m
- Recommended move
- Least recommended m

Para realizar un ataque de Golden Ticket es necesario haber obtenido:

- Nombre del dominio de destino.
- Nombre del usuario para suplantar.
- SID del dominio de destino.
- Hash de autenticación de kerberos del directorio activo.



Jugada 10

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Juega Superusuario

Tomar una decisión estratégica frente al ataque anterior.

Elija las acciones que aplicadas en combinación, prevendría el ataque de Golden Ticket, librando a la empresa SUPERUSUARIO de un golpe fatal que le sacaría de base y le haría perder el juego. Debes escoger todas las que apliquen, para que la jugada pueda ser válida:

- Utilizar aislamiento de sesiones para prevenir el residuo de credenciales en los equipos.
- Habilitar en el FW, la opción deep inspection package
- Utilizar limite de credenciales con aislamiento de sesiones para limitar el alcance del atacante.
- Colocar una DMZ.
- Hacer cumplir el acceso Just In Time (JIT) para minimizar los privilegios permanentes.


VICTORY!
Black's king can not escape check.
Play Again
JAQUEMATE
6. Nh4 Nxe4
7. Oh5 g6
8. BxF7+ KxF7
9. Oxg6+ Ke7
10. NF5#

Felicidades

Juntos Pudimos Tomar Mejores Desiciones


¡FELICIDADES!
GANADORES