Guatemala, 24 de marzo del 2023

ACT-003-EH-MIDES

ACTA DE REUNIÓN DE AVANCES DE LA CONSULTORÍA DE ETHICAL HACKING - SEMANA 3
(20 al 24 de marzo)

Acorde a lo establecido con el Ministerio de Desarrollo Social de Guatemala (MIDES), el día 24 de marzo de 2023 se realizó la segunda reunión de revisión de los avances de la **CONSULTORÍA DE ETHICAL HACKING**, cuyo objetivo es "Realizar el servicio de Ethical Hacking, tipo caja gris, sobre los activos considerados dentro el alcance en la red externa del Ministerio de Desarrollo Social de Guatemala, con la finalidad de evaluar la infraestructura externa de la institución y de esta manera identificar vulnerabilidades que podría permitir afectar potencialmente a la confidencialidad, integridad y disponibilidad de la información." reunión en la cual, se trataron los siguientes temas respecto a la ejecución del cronograma:

1. Alcance del proyecto
2. Cronograma del proyecto
3. Cumplimiento del proyecto
4. Siguientes pasos
5. Consideraciones generales

Se manifiesta el pleno cumplimiento del cronograma, manteniendo esta semana la ejecución de la fase de intrusión y explotación controlada, la identificación de dominios internos que estén asociados a la organización, la validación de las cuentas de usuarios en la deep y dark web, así como también la revisión de la deep y dark.

Los siguientes pasos a ejecutar la semana que viene corresponden a la realización del informe técnico.

Se destaca ciertas consideraciones obtenidas a partir del análisis al alcance enviado, su detalle a continuación:

IPs

No.	IPS	Alcanzable	Observación
1	190.61.97.134	Si	Sin contenido
2	190.61.97.136	No	No se evidencia sitio web
3	168.194.73.11	No	No se evidencia sitio web
4	168.194.73.12	Si	Sin contenido
5	168.194.73.8	Si	Sin contenido
6	168.194.73.15	Si	Manage Engine
7	168.194.73.24	Si	IIS
8	168.194.73.10	Si	IIS
9	190.61.97.146	No	No se evidencia sitio web
10	168.194.73.16	Si	Página principal
11	168.194.73.19	No	No se evidencia sitio web
12	168.194.73.14	Si	Pentaho
13	190.61.97.147	Si	SNIS
14	168.194.73.23	Si	WsSincronizar
15	168.194.73.27	Si	IIS

Web services:

N°	APLICACIONES	Alcanzable	WAF	Observación	IP
1	almacen.mides.gob.gt.	Si	CloudFlare	NA	104.22.65.182
2	antivirus.mides.gob.gt.	Si	-	NA	190.61.97.150
3	apirsh.mides.gob.gt.	No	-	No es alcanzable ni localmente, ni por vpn, ni desde guatemala	168.194.73.19
4	barracuda.mides.gob.gt.	No	-	No es alcanzable ni localmente, ni por vpn, ni desde guatemala	190.61.97.136
5	comedores.mides.gob.gt.	Si	CloudFlare	NA	104.22.65.182
6	sips.mides.gob.gt.	Si	-	NA	168.194.73.24
7	filessijdes.mides.gob.gt.	Si	-	NA	168.194.73.12
8	formularios.mides.gob.gt.	Si	CloudFlare	NA	172.67.11.245
9	sarh.mides.gob.gt.	Si	-	NA	168.194.73.8
10	mail.mides.gob.gt.	Si	-	NA	190.61.97.136

N°	Nombre	Sitio	Alcanzable	WAF	Observación	IP
1	becaempleo	becaempleo.mides.gob.gt.	Si	CloudFlare	NA	104.22.64.182
2	jovenes	jovenes.mides.gob.gt.	Si	CloudFlare	NA	172.67.11.245
3	adminrsh	adminrsh.mides.gob.gt.	No	-	No es alcanzable ni localmente, ni por vpn, ni desde guatemala	168.194.73.19
4	apirshdatos	apirshdatos.mides.gob.gt.	No	-	No es alcanzable ni localmente, ni por vpn, ni desde guatemala	168.194.73.19
5	rsh	rsh.mides.gob.gt.	No	-	NA	190.61.97.147
6	rsiso	rsiso.mides.gob.gt.	No	-	NA	168.194.73.19
7	sfi	sfi.mides.gob.gt.	Si	CloudFlare	NA	172.67.11.245
8	snis	snis.mides.gob.gt.	Si	-	NA	168.194.73.19
9	ssnis	ssnis.mides.gob.gt.	No	-	NA	168.194.73.19

De esta manera la reunión concluye con las siguientes consideraciones:

- Se ha cumplido con las fases de explotación y detección de filtraciones y se procede a continuar la fase desarrollo de informes, confirmando que la ejecución y entrega del proyecto se realizará en los tiempos determinados.
- Se ha evidenciado que no todos los activos del alcance se encuentran en línea.
- El equipo consultor hará una revisión de la zona de dominio para verificar que existan subdominios que, sin haber estado declarados en el alcance, se los pueda agregar en el proyecto.
- Se detectó una filtración de las cuentas ogarrido y cordones con el dominio mides.gob.gt. En el caso de que sean usuarios activos, se recomienda cambiar la contraseña inmediatamente.

Dejan constancia de lo antes expuesto:

Ministerio de Desarrollo Social de Guatemala.:

Orion Security Latam:

Firmado electrónicamente por:
JUAN CARLOS IZQUIERDO LARA

Ing. René Mazariegos
Administrador del Contrato
Ministerio de Desarrollo Social de Guatemala

Ing. Juan Carlos Izquierdo
Consultor de Proyecto
ORION SECURITY LATAM

Aprobado por parte de
Ministerio de Desarrollo Social de Guatemala.:

Firmado digitalmente por Eddy Noe Guzmán Orozco / 82633622

Ing. Eddy Guzmán
Director de Informática
Ministerio de Desarrollo Social de Guatemala