Universidad Autónoma de Yucatán

Licenciatura en Ingeniería de Software

Asignatura:

Ethical Hacking

Práctica 1: Maltego

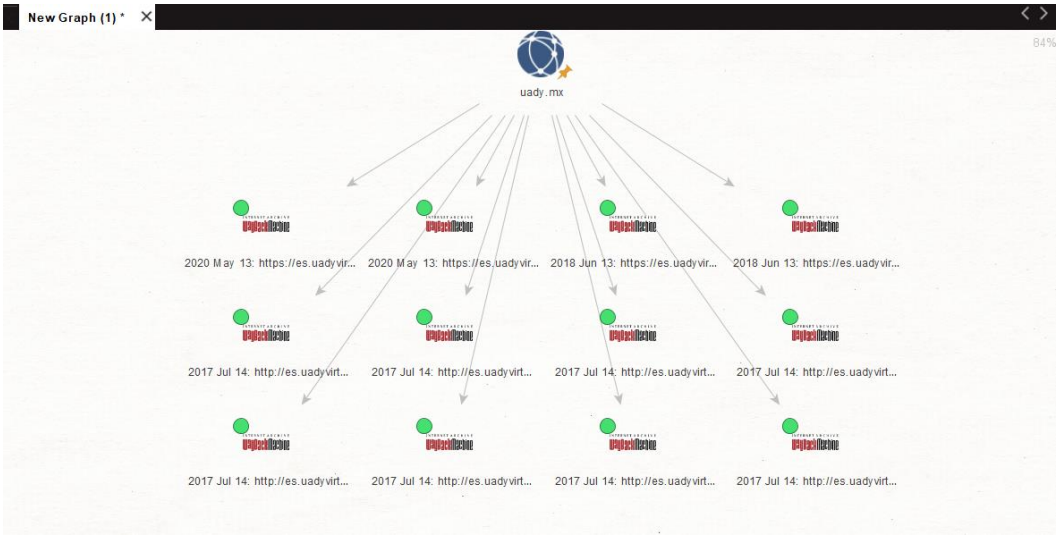
Alumno:

Alexis de Jesús Rosaldo Pacheco

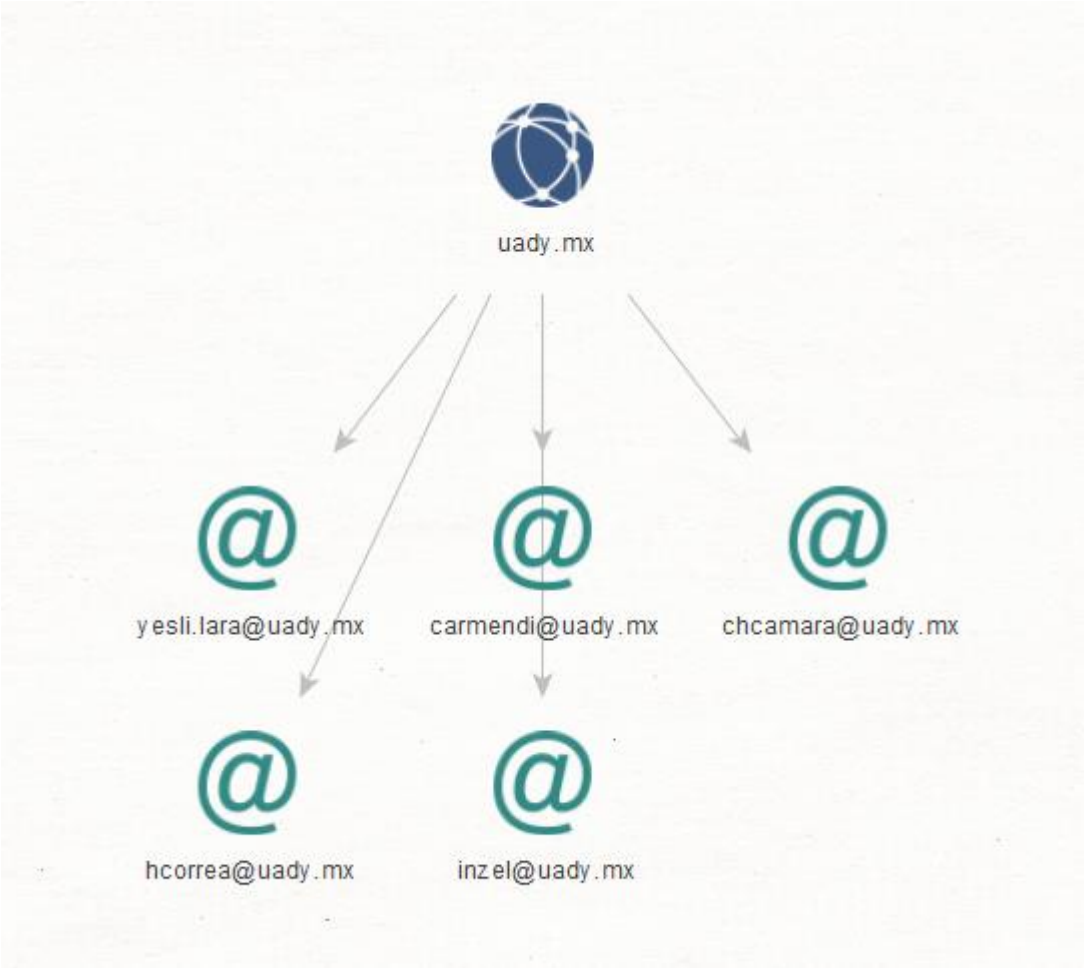
Profesor:

Pastor Enrique Góngora Cárdenas

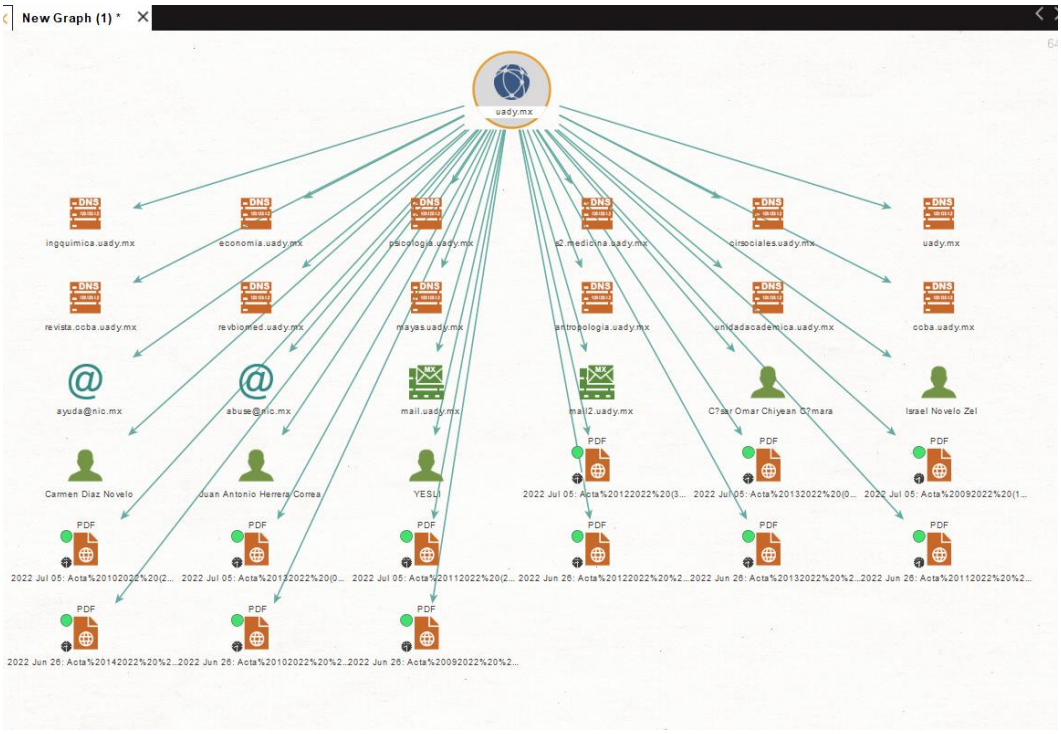
- **Screenshot de los gráficos obtenidos**
- **¿qué información arrojó maltego del dominio uady.mx?**



La primera captura provee información de versiones archivadas del sitio web asociado con la entidad "uady.mx", lo cual puede ser útil para identificar patrones de versiones y fechas y ver como lucía el sitio en esas fechas(desde 1970 hasta actualidad) y ver la información que contenía y era pública.



La segunda captura provee nombres de contactos de correo electrónico púbicos.



La última captura incluye información de correos de contacto de la uady, nombres de personas públicos, también indica las distintas DNS las cuales están relacionadas con el dominio de la uady e información/enlaces de e-mails y documentos encontrados en los sitios, al igual que IPs que sean públicas.

Si fueras hacker de sobrero negro ¿para qué te sería útil maltego?

Podría localizar información de los nombres de dominios de algún sitio y comenzar a recabar información de dicho sitio o organización es específico que sea pública, por ejemplo:

- Dominios y subdominios asociados.
- Documentos en los distintos dominios.
- Correos electrónicos dentro del sitio.
- IPs que puedan estar púbicos.
- Contactos, correos, números de teléfono, etc..., de personas que estén públicos en los sitios o documentos asociados a los mismos.
- Información que haya estado pública en el pasado y que ahora ya no lo es mediante el los snapshots.

Como hacker de sombrero blanco ¿qué sugieres hacer para mitigar el riesgo de que un pirata use maltego en su beneficio?

-
- Realiza auditorías periódicas para asegurarte de que no existan subdominios inactivos o vulnerables.
- Ofuscar correos electrónicos y datos sensibles usando java script o algún framework que evite poner información completa de correos
- Configurar un archivo robots.txt restrictivo para motores de búsqueda.
- Proteger documentos y directorios desactivando directorios con información sensible y solicitando autentificación para aquellos que si lo requiera.
- Solicitar eliminación en Wayback Machine para eliminar snapshots que contengan información sensible
- Monitorear y eliminar subdominios inactivos o vulnerables.
- Implementar cabeceras de seguridad como Content-Security-Policy y X-Frame-Options para proteger el sitio.
- Bloquear bots maliciosos mediante herramientas como Cloudflare o reCAPTCHA para evitar la recolección automatizada de información.