

PRACTICA 1

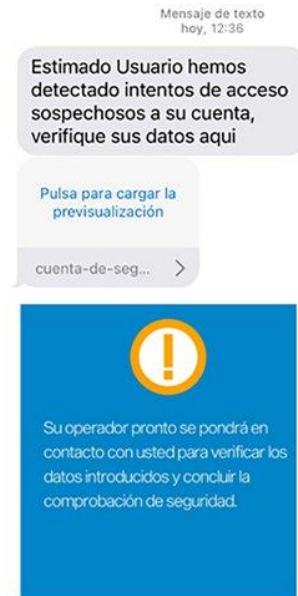
Daniel Khomyakov Trubnikov

TEMA 1:

- Buscar y analizar dos ataques importantes que hayan sido realizados durante los años 2020-2021. Uno de ellos debe haber tenido por objetivo el sabotaje o espionaje, y otro el robo masivo de cuentas o fines monetarios. Se debe de indicar al menos el método de ataque utilizado, objetivos del ataque, países afectados y tiempo de actividad.

Los ataques de los cuales voy a hablar van a ser sobre los de robo de datos/espionaje respecto a las vacunas de COVID-19 entre distintos países y luego un robo masivo de cuentas bancarias. Sobre las vacunas COVID -19 se ve que distintos países intentan robar información o hasta sabotear la distribución de estas mismas, pero también el robar datos sanitarios los cuales luego junto a todo lo anterior se podría usar para extorsionar a los países afectados. Para dar un ejemplo claro, en noviembre del 2020 un grupo de hackers norcoreanos llamado Lazarus intento distribuir software malicioso a los empleados de una productora de vacunas COVID-19 británica llamada AstraZeneca y Oxford e intentaros ocultaron dicho software malicioso con falsas ofertas de trabajo a través de LinkedIn u WhatsApp.

Ahora hablaré sobre los ataques de las cuentas bancarias que sucedido en España donde un grupo de hackers no identificado ha estado pasándose por entidades bancarias en las cuales hacían pedir a las víctimas que se registrasen en una página web falsa del banco de la víctima en la cual se pediría que introdujese datos sensibles de la cuenta bancaria a través de un SMS con un enlace al banco y con el siguiente mensaje: *“Hemos detectado intentos de acceso sospechosos a su cuenta. Debe activar su sistema de seguridad web o bien su cuenta quedará bloqueada”*. Una vez conseguidos dichos datos, los atacantes proceden a realizar llamadas de las victimas con el objetivo de llevar a cabo transacciones falsas de la cuenta bancaria de la víctima para conseguir su dinero. La siguiente imagen muestra dicho Tweet sacado por la Policía Nacional avisando así que las personas no caigan en la trampa de los ciberataques.



Si nos fijamos en ambos casos se han llevado a cabo con el uso del phishing donde en el primer caso los atacantes se hacían pasar por reclutadores de personal mientras que en el otro caso por identidades bancarias.

- Buscar información sobre las acciones y programas de espionaje de la NSA. Analizar las técnicas, procedimientos y colaboraciones realizadas. Analizar posteriormente dos proyectos a elección del alumno que se encuentren dentro del catálogo ANT TAO de la NSA, destacando los detalles de los mismos.

La NSA (o ANS en español que se refiere a Agencia Nacional de Seguridad) se trata de un grupo americano que se ocupa de recopilar y espionaje de datos de manera global para conseguir información respecto a lo que ocurre tanto dentro como fuera del país. Las colaboraciones principales que tiene son con casi todo lo que está vinculado U.S. ya sean sus aliados, agencias industriales como lo presentare como un ejemplo más adelante.

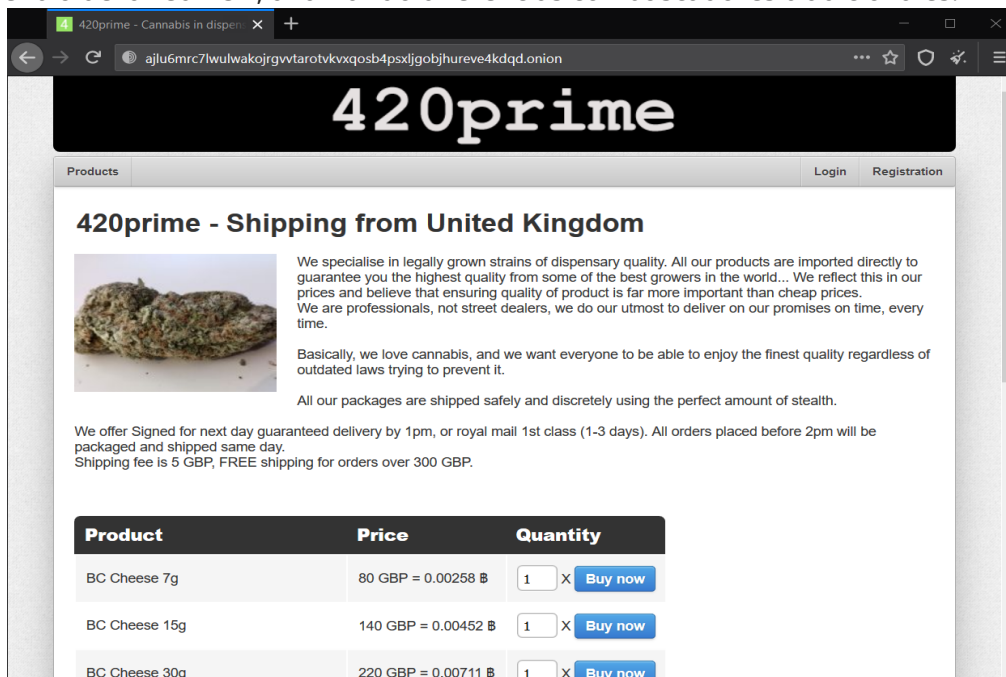
PRISM se trata de un programa Estado Unido perteneciente a la NSA el cual se ocupa de espiar a sus ciudadanos donde el programa tiene un acceso directo a todos los servidores de EU, por lo que incluye acceso a los servidores de compañías multimillonarias como Apple, Microsoft, Google ... Como podemos ver en este ejemplo, a lo mencionado anteriormente podemos ver como gracias a las colaboraciones que tiene con el Gobierno de Estados Unidos puede NSA realizar dicha acción sobre estas compañías.

Ahora el catálogo de ANT TAO es uno que fue creado por Der Speilg con el propósito de que trabajadores del NSA puedan pedir dichas tecnologías que propone como si fuese un pedido de Amazon, por ejemplo. Los dos proyectos de los cuales voy a estar hablando serán IRONCHEF y HEADWATER teniendo estos una cosa en común es que el objetivo de los dos es infectar a los sistemas objetivos, pero a su manera.

En el caso de IRONCHEF se trata de obtener un acceso eterno a sistema del objetivo con el uso de la motherboard BIOS y luego pues usando el SMM para comunicarte con los componentes del sistema mediante un implante en el HW que mencione antes. De esta manera uno puede controlar el ordenador (como ejemplo) desde sus componentes haciendo que este mismo este a total disposición del IRONCHEF sin que el usuario del ordenador pueda hacer algo, acaso que sea cambiar los componentes hardware de su ordenador por unos propios. También junto al IRONCHEF se instala un implante SW CNE para acompañar el IRONCHEF, pero también si se desinstala el implante de SW CNE pues el IRONCHEF se asegura de porque ha sido esto y luego lo vuelve a reinstalar.

Por otro lado, está el HEADWATER el cual mete otro implante llamado PBD el cual solo afectaba a los sistemas Huawei mediante sus rúters. El objetivo de este implante es poder hacer acciones o funciones y obligar a que el Huawei afectado las realice a través de la red sin tener que estar delante del dispositivo y poder usarlo o con la adición de un HW específico como en el ejemplo anterior del IRONCHEF. Para la instalación del PBD también se hace mediante la red, el cual, una vez instalado junto a otros operadores, el PBD podrá interceptar cual sistema proxy todos los paquetes que pasen por el rúter (aparte de mandar funciones específicas a realizar como mencioné antes).

- Instalar y hacer uso de TOR para acceder a la 'Deep Web'. Identificar buscadores web dentro de la red TOR, analizando diferencias con buscadores tradicionales.



420prime

Products Login Registration

420prime - Shipping from United Kingdom

We specialise in legally grown strains of dispensary quality. All our products are imported directly to guarantee you the highest quality from some of the best growers in the world... We reflect this in our prices and believe that ensuring quality of product is far more important than cheap prices. We are professionals, not street dealers, we do our utmost to deliver on our promises on time, every time.

Basically, we love cannabis, and we want everyone to be able to enjoy the finest quality regardless of outdated laws trying to prevent it.

All our packages are shipped safely and discretely using the perfect amount of stealth.

We offer Signed for next day guaranteed delivery by 1pm, or royal mail 1st class (1-3 days). All orders placed before 2pm will be packaged and shipped same day.
Shipping fee is 5 GBP, FREE shipping for orders over 300 GBP.

Product	Price	Quantity
BC Cheese 7g	80 GBP = 0.00258 ₿	1 X Buy now
BC Cheese 15g	140 GBP = 0.00452 ₿	1 X Buy now
BC Cheese 30g	220 GBP = 0.00711 ₿	1 X Buy now

Cuando hablamos de la Deep web he encontrado que realmente hay 3 términos que hay que tener en cuenta, la Clearnet, la Deep Web y la Dark Web yendo en este orden de visibilidad. La Clearnet tratándose de todas esas páginas las cuales se puede acceder de manera rápida y sin problema como Google, Yahoo! y etc. La Deep Web son aquellas las cuales páginas están detrás de algo que no cualquiera puede acceder, como un paywall y no se puede acceder de manera pública es esta misma y otro ejemplo serio como un Dropbox. En este caso estaremos viendo la Dark Web la cual está dentro de la Deep Web donde los buscadores en vez de terminar en un .com, .es, .net y otros por el estilo, termina en un .onion como en este caso junto como a muchísimos caracteres los cuales no tiene que ver entre sí, es decir, no es un www.Google.com donde sabes que el enlace tiene que ver con Google, donde en mi imagen podemos ver que se trata de una venta de Cannabis y la URL no tiene nada que ver con Cannabis en sí. En este caso al estar hablando de TOR, estas URL se generan de manera un poco aleatoria usando el método de encriptación de RSA de 1024 bits para cifrarlo y junto a esto se calcula luego el SHA-1 usando un trozo de la clave pública. Con todo esto se terminan creando capas y capas de cifrado para hacer que las páginas estas sean anónimas dentro del dominio .onion (capas como una cebolla).

Tema 2:

- Investigar las herramientas Open Source que pueden ser utilizadas para desplegar un honeypot en no más de una cara. Posteriormente el alumno deberá hacer uso de al menos una de dichas herramientas para montar un simple honeypot de baja interacción, y exponerlo a ser posible en Internet para comprobar si se generan alertas. Deberá ser descrito el proceso y los pasos seguidos, así como las alertas que hubieran sido detectadas.

Para la descarga y despliegue de honeypots existen de varios tipos, entre estos los de pago y los gratis (open Source) de los cuales gratis y hablara de ello son el Conpot y el Pentbox. El Conpot es un honey pot de servidor de baja iteración hecho de tal manera que sea fácil desplegarlo de tal manera que una vez instalado uno pueda modificarlo fácilmente para que sea como lo quiere el usuario. Con tanta versatilidad este mismo puede emular los sistemas honeypots de una empresa entera para ir probando y experimentando en unos sistemas propios para ver como seria el funcionamiento de esta misma sin tener que ver una en persona y hacer todas las pruebas que uno quiera sin restricciones. Por otro lado, está el Pentbox el cual quizás no sea específicamente usado para hacer honeypots, sí que es una de sus funciones y en la cual me voy a centrar ya que es lo que nos interesa, sobre todo ya que elegí esta herramienta para el levantamiento del honeypot. En un principio, el nombre de dicho programa hace referencia a que se hacen pruebas en esta misma para distintos usos, como crackeadores hash, creador de honeypot, generador de contraseñas seguras ante distintos ataques y muchos más. En este caso el honeypot que despliega el Pentbox también es de baja interacion ya que como podremos ver más adelante al activarse el honeypot, y me intento meter en la pagina de la ip de la maquina en la que tengo montado el honeypot, me lo bloqueo y me manda una señal de esa intrusión, aunque eso ahora lo enseñó en detalle con imágenes y explicando un poco el procedimiento.

Primero para la instalación de este mismo, nos descargamos la versión que haya desde la página de sourceforge donde descomprimos el .zip y procedemos a entrar en la carpeta para inicializar el pentbox el cual una vez encendido nos saldrá algo así:

```
daniel@daniel: ~/Documents/pentbox-1.8
File Actions Edit View Help
PentBox 1.8
  (oo)____
  ( )____) --*
  ||----||

Menu      ruby2.7.4 @ x86_64-linux-gnu
1- Cryptography tools
2- Network tools
3- Web
4- Ip grabber
5- Geolocation ip
6- Mass attack
7- License and contact
8- Exit

→ 2
```

Es importante anotar aquí como podemos ver a cerca del menú pone una cosa de Ruby, siendo esto el lenguaje de interpretación que se ha usado para su creación. Después de iniciar nos aparecerán varias opciones de las cuales como en la práctica se nos pidió exponer el honeypot en la red pues entramos en el network tools que sería la opción 2 de dicho programa.

```
daniel@daniel: ~/Documents/pentbox-1.8
File Actions Edit View Help
→ 2

1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)
0- Back

→ 3

// Honeypot //

You must run PentBox with root privileges.

Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

→ 1

HONEYPOT ACTIVATED ON PORT 80 (2021-10-05 11:18:39 +0200)
```

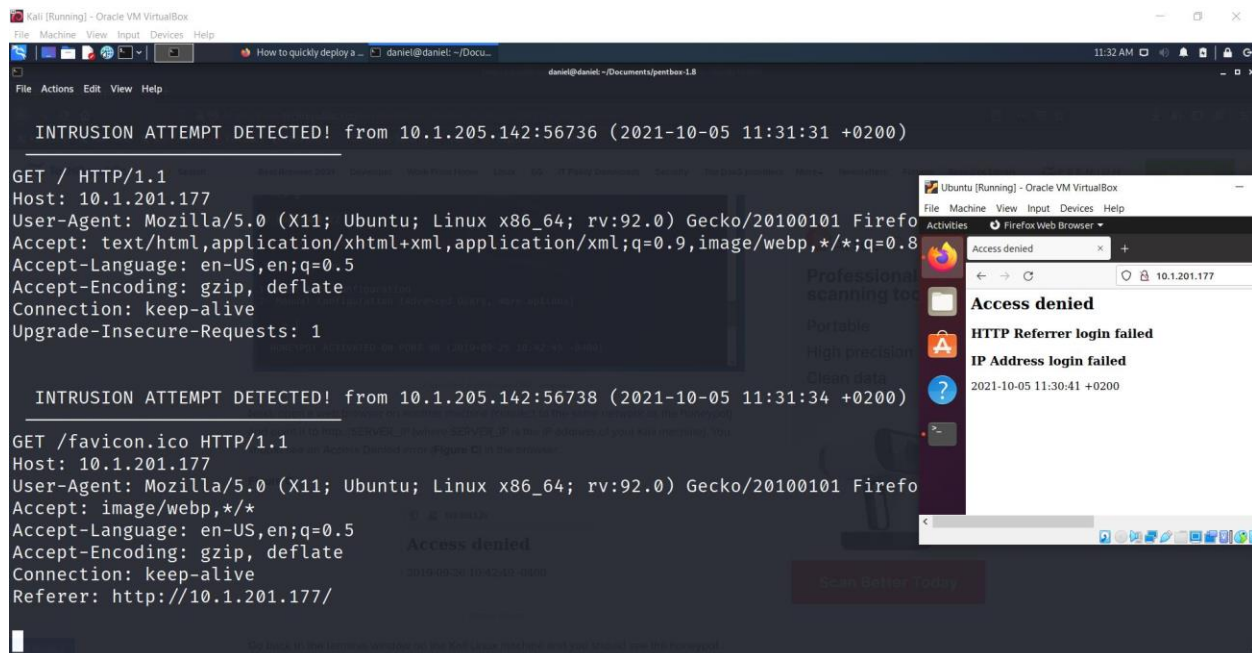
En esta parte podemos ver como después de entrar en esta opción nos aparece justo lo que queríamos que sería el despliegue del honeypot junto a otras opciones las cuales no les prestaremos atención ya que queremos desplegar el honeypot donde por ende le daremos a la opción 3. Una vez presionada la opción nos saldrá dos maneras para que sea desplegado, por un lado, la forma automática la cual para simplificar el asunto fue la que elegí, y luego la manual en la cual se podrá usar para desplegar dicho honeypot pero para puertos específicos por ejemplo u otras opciones. Pues cuando le di a la opción 1 pues se me configuro rápido y cómo podemos ver se me desplego en el puerto 80, el cual pertenece al servicio de http.

Ahora para demostrar que ha funcionado dicho honeypot primero presentare las IP de ambas maquinas:

```
(daniel@daniel) - [~/Documents/pentbox-1.8]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:14:71:10 brd ff:ff:ff:ff:ff:ff
    inet 10.1.201.177/21 brd 10.1.207.255 scope global dynamic noprefixroute eth0
        valid_lft 21294sec preferred_lft 21294sec
    inet6 fe80::a00:27ff:fe14:7110/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
danekar@danekar: ~
danekar@danekar:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:9c:d6:6e brd ff:ff:ff:ff:ff:ff
    inet 10.1.205.142/21 brd 10.1.207.255 scope global dynamic noprefixroute enp0s3
        valid_lft 3369sec preferred_lft 3369sec
    inet6 fe80::5752:e637:34fa:738/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
danekar@danekar:~$
```

En la primera imagen podemos ver la máquina de Kali que es donde tenemos desplegado el honeypot con la IP: 10.1.201.177 mientras que para la máquina de Ubuntu que será la cual intentará entrar en la página web de la IP de la maquina Kali con la IP suya de: 10.1.205.142. También un dato importante que tener en cuenta y es para que las maquinas puedan verse entre estas las puse en adaptador puente en VirtualBox para que estas pertenezcan a la misma red y ahora una vez establecido esto, podemos presenciar el ejemplo:



Como podemos ver, para empezar la máquina de Ubuntu es la cual está en miniatura a la derecha la cual al poner la ip de Kali pues podemos ver que nos niega el acceso como si hubiese un error de un tipo, mientras que en Kali podemos ver como el honeypot que desplegamos detecta dicha intrusión, y no solo nos avisa de esta misma que sino también nos dice de que IP sale que en este caso es la de Ubuntu ya que es la que intento meterse en la página web (que es http por tanto el puerto 80 el cual le dijimos al honeypot) del Kali.

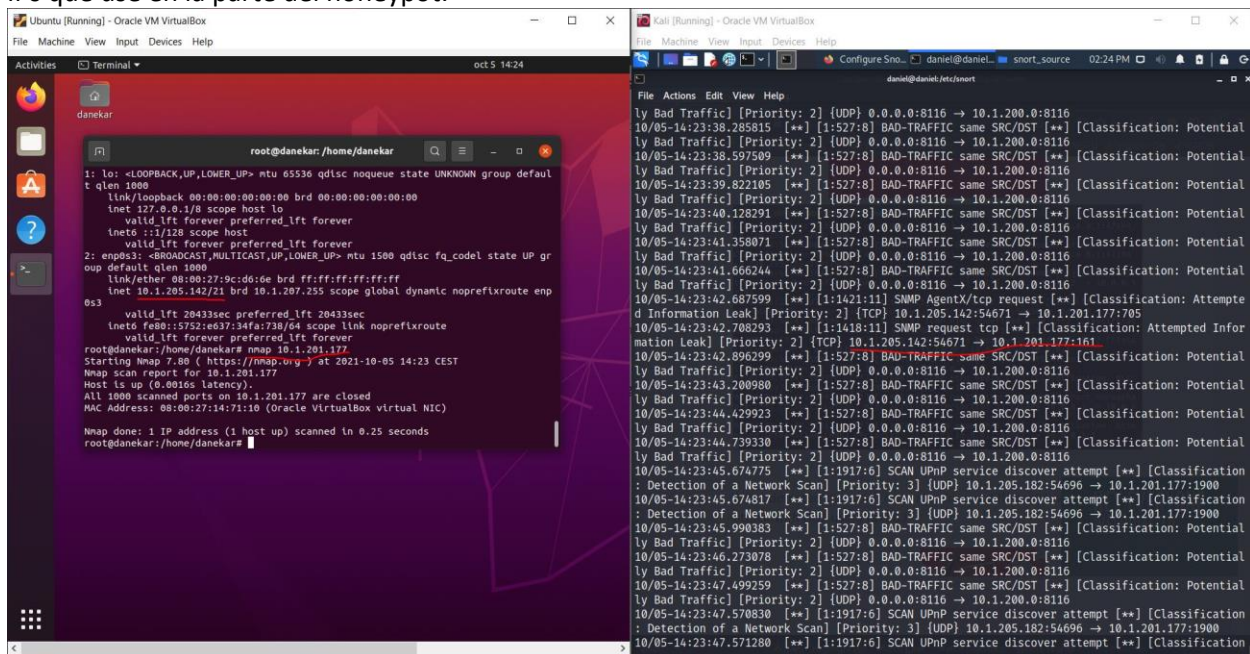
- Analizar los usos de Snort, y desplegarlo como IDS de red. Se deberá realizar un resumen de donde se encuentra las firmas que utiliza, y explicar el funcionamiento de al menos 2 de ellas, mostrando además el proceso de explotación o pruebas que ha sido realizado.

El snort es un IDS, el cual significa que es un sistema de detección de intrusos en la red. Este es un sistema el cual permite monitorizar de manera constante lo que ocurre en la red y además especificarle unas firmas/reglas las cuales la red debe seguir o acciones que hacer en caso de que una de estas no se cumple. Como mencione antes, nos permite ver de manera constante lo que ocurre en la red, por lo tanto podemos definirlo como un sniffer y ver en la consola que cosas están ocurriendo a tiempo real, de si hay una intrusión o no y luego guardar dicha información que sale por consola (que es una motorización de paquetes como si fuese un Wireshark) y guardarla en una especie de log para verlo más tarde en detalle si hace falta. Cuando algunos de los paquetes que se envía de manera constante choca con algunas de las firmas que establecimos, pues se puede ver como este mismo lo detecta.


```
File Actions Edit View Help
(daniel@daniel)-[/etc/snort/rules]
$ ls
attack-responses.rules      community-smtp.rules        icmp.rules                  shellcode.rules
backdoor.rules              community-sql-injection.rules  imap.rules                 smtp.rules
bad-traffic.rules           community-virus.rules        info.rules                  snmp.rules
chat.rules                  community-web-attacks.rules   local.rules                 sql.rules
community-bot.rules         community-web-cgi.rules       misc.rules                  telnet.rules
community-deleted.rules     community-web-client.rules    multimedia.rules            tftp.rules
community-dos.rules         community-web-dos.rules       mysql.rules                 virus.rules
community-exploit.rules     community-web-iis.rules       netbios.rules               web-attacks.rules
community-ftp.rules         community-web-misc.rules       nntp.rules                  web-cgi.rules
community-game.rules        community-web-php.rules       oracle.rules                 web-client.rules
community-icmp.rules        deleted.rules                 other-ids.rules              web-coldfusion.rules
community-imap.rules        dns.rules                     p2p.rules                   web-frontpage.rules
community-inappropriate.rules  dos.rules                    policy.rules                 web-iis.rules
community-mail-client.rules  experimental.rules            pop2.rules                   web-misc.rules
community-misc.rules         exploit.rules                  pop3.rules                   web-php.rules
community-nntp.rules         finger.rules                   porn.rules                   x11.rules
community-oracle.rules       ftp.rules                      rpc.rules                    rservices.rules
community-policy.rules       icmp-info.rules               scan.rules
```

Para ver donde están las firmas que se aplican en el snort pues nos tenemos que meter en la siguiente dirección: `cd /etc/snort/rules` y allí podremos ver todas las reglas definidas en el snort que como podemos ver por defecto viene bastantes de estas. Para explicar dos de estas elegiré la de icmp y el backdoor donde empezando por la segunda, backdoor se trata de la detección de un programa maligno el cual trata de traquear en el caso en el cual pasen muchísimos datos de una maquina infectada los cuales generan un gran tráfico de en la comunicación en la red. Por otro lado, está el icmp el cual simplemente es detectado cuando vienen señales de pines de unas herramientas que se usa para atacar a las redes.

Para mostrar cómo funciona dicho sistema, mostraré un ejemplo que realicé con las mismas maquinas y IPs que usé en la parte del honeypot.



```
File Machine View Input Devices Help
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Configure Snort... daniel@daniel... snort_source 02:24 PM
daniel@daniel:~$ snort -t
File Actions Edit View Help
ly Bad Traffic [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:38.285815 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:38.597509 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:39.822105 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:40.128291 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:41.358071 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:41.666244 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:42.687599 [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempte
d Information Leak] [Priority: 2] [TCP] 10.1.205.142:54671 -> 10.1.201.177:705
10/05-14:23:42.708293 [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Infor
mation Leak] [Priority: 2] [TCP] 10.1.205.142:54671 -> 10.1.201.177:705
10/05-14:23:42.896299 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:43.200980 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:44.429923 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:44.739330 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:45.674775 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification
: Detection of a Network Scan] [Priority: 3] [UDP] 10.1.205.182:54696 -> 10.1.201.177:1900
10/05-14:23:45.674817 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification
: Detection of a Network Scan] [Priority: 3] [UDP] 10.1.205.182:54696 -> 10.1.201.177:1900
10/05-14:23:45.900383 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:46.273078 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:47.499259 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potential
ly Bad Traffic] [Priority: 2] [UDP] 0.0.0.0:8116 -> 10.1.200.0:8116
10/05-14:23:47.570830 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification
: Detection of a Network Scan] [Priority: 3] [UDP] 10.1.205.182:54696 -> 10.1.201.177:1900
10/05-14:23:47.571280 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification
```

Como podemos observar pues en la parte de la derecha se ve como active el snort y empieza a actuar como un sniffer rastreando cada paquete y comprobado este mismo y a la izquierda está el Ubuntu el

cual al principio solo hago un "IP a" para mostrar la IP de este mismo. Una vez que se demuestra las máquinas que uso, podemos ver como en la máquina de Ubuntu realizo un simple nmap sobre la máquina de Kali para ver que puertos o servicios tiene abiertos y podemos ver como el snort lo ha detectado dándonos datos importantes como que tipo de regla fue afectada que es la SNMP, junto a qué tipo de transferencia de paquetes hace (que es el TCP en este caso) y además de que IP a cual se realizó dicho análisis. Además, también nos clasifica que este tipo de ataque ha podido haber sido de intento de robo de información que en este caso lo ha sido pudiendo yo ver si esta máquina tiene algún tipo de servicio que me interese.

- Investigar los diferentes usos de un MDM en la actualidad dentro de una organización, y realizar un resumen de los mismos que indique las funcionalidades y características principales. El alumno deberá analizar al menos un fabricante / proveedor, y comprobar cuales de las funcionalidades principales cumple, y que características adicionales tiene.

La idea general del MDM (Mobile Device Management) en una compañía es para mejorar el desempeño de los empleados sin comprometer la seguridad de la empresa que usa dicho sistema. Esto mismo les permite hacer uso de muchos aparatos electrónicos y entre estos pues diferentes sistemas operativos donde los equipos de IT pueden monitorizar los dispositivos que se usen en la empresa, así pues, aplicando la idea que dije anteriormente manteniendo así pues la seguridad del lugar junto a la gran conexión que hay entre los dispositivos de los trabajadores.

Para el proveedor he escogido el Scalefusion, cumple las funciones básicas de un MDM, donde los sistemas operativos que cubre son Android, IOS y macOS y con esto le da la oportunidad de dejar a las empresas si quieren que sus empleados usen aparatos que les proporciona la empresa, o según la metodología BYOD (Bring Your Own Device) que se trata de que los empleados se traigan sus propios aparatos electrónicos que contengan alguno de los sistemas operativos mencionado anteriormente. Como detalle extra ofrecen una demo de su MDM o a lo mejor para poder disponer de todas sus disposiciones pues también ofrece un free-trial en el cual se puede usar todo lo que ofrece el proveedor.

Cosas nuevas las cuales añade esta MDM es la manipulación de dispositivos a distancia, es decir, todos los dispositivos que estén conectados al MDM pues pueden ser no solo monitoreados por el equipo encargado de la seguridad de la compañía, sino que también manipular estos mismos para que hagan distintas funciones. Si lo ponemos así hasta un punto suena como un programa maligno, pero al igual como en el catálogo de NSA ATO, en el cual uno de los cuales analicé el HEADWATER el cual se encargaba de hacer algo parecido, pero solo con los dispositivos Huawei, pero en este caso son para aumentar la seguridad de la empresa. Entre otras cosas que añaden además la localización a tiempo real de todos sus dispositivos y la restricción de los correos electrónicos visibles para distintos usuarios y con esto último me refiero a que si digamos que existen 5 buzones donde llegan distintos correos electrónicos y cada buzón está especializado para un tipo de correo específico. Pues con esto quizás a los empleados que sean más nuevos no tendría sentido que viesen los datos confidenciales de la empresa, pues solo tendría sentido que estos recibiesen correo de solo un buzón, mientras que los del equipo de IT los cuales monitorizan todo esto, pues pueden ver los 5 y mirar que tipo de correo está llegando a cada uno.

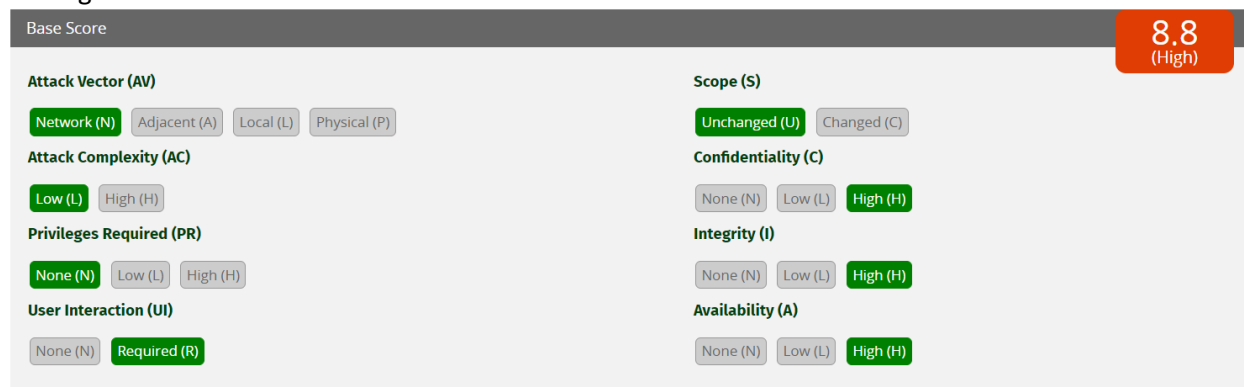
TEMA 3:

- Seleccionar dos grupos cibercriminales de los clasificados en Mitre ATT&CK y analizar en que consisten las principales técnicas utilizadas. Para al menos 5 técnicas se deberá calcular el CVSS asociado a la vulnerabilidad que explotan y el impacto que tendría sobre una organización.

Dentro de la página oficial de Mitre ATT&CK pues nos encontramos con bastantes opciones de las cuales seleccioné fueron la Inicial Access y Defence Evasion siendo estas dos un tanto que complementarias hasta un punto según mi opinión. Con lo último que dije me refiero a que en Inicial Access se trata de conseguir acceso a la red de una forma u otra, ya sea a través de los empleados como en el ejemplo que di de la parte 1 de esta práctica como en el ejemplo de AstraZeneca donde unos hackers norcoreanos intentaron conseguir acceso a la red de esta compañía mediante una de las técnicas mencionadas en este grupo (Inicial Access me refiero) que es el phishing. Esto también es importante entender que los métodos que se emplean en este grupo a parte del phishing son para luego seguir accediendo a más adentro de la organización para recabar más datos, hacer más daño a la empresa en cuestión o etc. Luego en la parte de Defence Evasion es un poco como el nombre indica, evadir las defensas del lugar mediante técnicas de desactivación de estas mismas o que los software maliciosos pasen desapercibidos y hasta un punto si lo pensamos, se están evadiendo estas defensas en el Inicial Access con algunos métodos como el de phishing, aunque ese sea a través de los empleados de una empresa por ejemplo y de ahí que los relaciono un poco aunque entiendo que la parte de Defence Evasion se trata sobre todo de pasar software malicioso a través de las defensas, desactivar estas mismas o hacer que hagan otras cosas como que los atacantes las usen en su beneficio.

Para la siguiente parte estas serán las 5 tecnicas de las cuales les voy a calcular el CVSS y pondré capturas como respuestas a estas: Phising, Exploit Public-Facing Application, Abuse Elevation Mechanism, Deploy Container, Masquerading.

Phising:



Category	Options	Selected
Attack Vector (AV)	Network (N), Adjacent (A), Local (L), Physical (P)	Network (N)
Attack Complexity (AC)	Low (L), High (H)	Low (L)
Privileges Required (PR)	None (N), Low (L), High (H)	None (N)
User Interaction (UI)	None (N), Required (R)	Required (R)
Scope (S)	Unchanged (U), Changed (C)	Unchanged (U)
Confidentiality (C)	None (N), Low (L), High (H)	High (H)
Integrity (I)	None (N), Low (L), High (H)	High (H)
Availability (A)	None (N), Low (L), High (H)	High (H)

Base Score: 8.8 (High)

En este caso las tres primeras opciones son un poquito más obvias, luego es importante que el usuario interactúa con el mensaje malicioso para que se le pueda sacar información a ese mismo donde obviamente el objetivo seguirá siendo el mismo si se trata de un ataque a una empresa pues se entiende que los objetivos serán los empleados y seguirán siéndolo. Por otro lado, tenemos los casos de confidencialidad donde es normal que sea alta la pérdida ya que en caso de que se cumpla el ataque, pues eso significa que el usuario ha dado alguno de sus datos y ha sido “pescado”. Por ende, como el atacante tiene acceso a los datos de la víctima, pues dependiendo los datos que se le han pasado siendo contraseñas

de usuario lo típico, pues la integridad estará igual de mal ya que eso le permite al atacante modificar lo que quiere. Por último, la viabilidad si se llega a ser el usuario root de algún empleado que tiene control sobre los demás es perfectamente capaz de bloquearles acceso a esos usuarios o a la víctima en si también haciendo un cambio de contraseña por ejemplo.

Exploit Public-Facing Application:

Base Score		8.2 (High)
Attack Vector (AV)	Scope (S)	
<input checked="" type="radio"/> Network (N) <input type="radio"/> Adjacent (A) <input type="radio"/> Local (L) <input type="radio"/> Physical (P)	<input checked="" type="radio"/> Unchanged (U) <input type="radio"/> Changed (C)	
Attack Complexity (AC)	Confidentiality (C)	
<input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)	<input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)	
Privileges Required (PR)	Integrity (I)	
<input checked="" type="radio"/> None (N) <input type="radio"/> Low (L) <input type="radio"/> High (H)	<input type="radio"/> None (N) <input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)	
User Interaction (UI)	Availability (A)	
<input checked="" type="radio"/> None (N) <input type="radio"/> Required (R)	<input checked="" type="radio"/> None (N) <input type="radio"/> Low (L) <input type="radio"/> High (H)	

Base Score		9.1 (Critical)
Attack Vector (AV)	Scope (S)	
<input checked="" type="radio"/> Network (N) <input type="radio"/> Adjacent (A) <input type="radio"/> Local (L) <input type="radio"/> Physical (P)	<input checked="" type="radio"/> Unchanged (U) <input type="radio"/> Changed (C)	
Attack Complexity (AC)	Confidentiality (C)	
<input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)	<input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)	
Privileges Required (PR)	Integrity (I)	
<input checked="" type="radio"/> None (N) <input type="radio"/> Low (L) <input type="radio"/> High (H)	<input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)	
User Interaction (UI)	Availability (A)	
<input checked="" type="radio"/> None (N) <input type="radio"/> Required (R)	<input checked="" type="radio"/> None (N) <input type="radio"/> Low (L) <input type="radio"/> High (H)	

Aquí pues pongo dos imágenes porque pienso que es importante remarcar las diferencias en ambos casos. Por un lado, tenemos la primera con un 8,3 donde la diferencia entre las dos es que en la primera no la integridad la pongo en bajo y en el otro en alto y esto se debe a que estas técnicas son de aprovechar las vulnerabilidades de una página web por ejemplo para poder meterse dentro ya sea con el uso de comandos, data o programas exteriores ya que la pagina tenga una vulnerabilidad, un glitch, bug y etc. Asique como además probamos hacer este tipo ataque, sabemos que podemos llegar a sacar las contraseñas de los usuarios como sus nombres u otros datos, pero lo que es importante que quizás con una técnica mas avanzada de esto mismo uno podría hasta modificarlos, de ahí que decidí dejar dos imágenes.

Abuse Elevation Control Mechanism:

Base Score		7.4 (High)
Attack Vector (AV) Network (N) Adjacent (A) Local (L) Physical (P)	Scope (S) Unchanged (U) Changed (C)	
Attack Complexity (AC) Low (L) High (H)	Confidentiality (C) None (N) Low (L) High (H)	
Privileges Required (PR) None (N) Low (L) High (H)	Integrity (I) None (N) Low (L) High (H)	
User Interaction (UI) None (N) Required (R)	Availability (A) None (N) Low (L) High (H)	

Este ataque se trata de conseguir de una manera u otra el acceso a poder aumentarse los privilegios de uno mismo en el sistema sin tener conexión de ningún tipo con ninguna persona o extra. Es por esto por lo que yo también creo que la complejidad del ataque sería alta ya que intenta dentro del sistema solo para conseguir la forma de aumentarse los privilegios modificando el funcionamiento interno de este mismo. Mientras que por el otro lado como no se está intentando conseguir esto a través de otro usuario o algo, sino que solo aumentar los privilegios, pues entiendo que no se llega a perder la confidencialidad, aunque sí que es cierto que a través de esta mecánica se podría llegar a conseguir dichos datos.

Deploy Container:

Base Score		9.8 (Critical)
Attack Vector (AV) Network (N) Adjacent (A) Local (L) Physical (P)	Scope (S) Unchanged (U) Changed (C)	
Attack Complexity (AC) Low (L) High (H)	Confidentiality (C) None (N) Low (L) High (H)	
Privileges Required (PR) None (N) Low (L) High (H)	Integrity (I) None (N) Low (L) High (H)	
User Interaction (UI) None (N) Required (R)	Availability (A) None (N) Low (L) High (H)	

Tratándose de un ataque que es bastante simple donde el atacante intenta pues meter un “contenedor” que contiene software malicioso, y este puede estar en una imagen o directamente en un documento. Con esto el software malicioso tiene que misión burlar la seguridad del sitio otorgándole acceso directo al atacante en cuestión ya sea cambiando las reglas del iptables, cambiando las limitaciones del usuario o hasta los permisos y etc.

Masquerading:

Base Score		8.1 (High)
Attack Vector (AV) <input checked="" type="radio"/> Network (N) <input type="radio"/> Adjacent (A) <input type="radio"/> Local (L) <input type="radio"/> Physical (P)	Scope (S) <input checked="" type="radio"/> Unchanged (U) <input type="radio"/> Changed (C)	
Attack Complexity (AC) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)	Confidentiality (C) <input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)	
Privileges Required (PR) <input checked="" type="radio"/> None (N) <input type="radio"/> Low (L) <input type="radio"/> High (H)	Integrity (I) <input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)	
User Interaction (UI) <input checked="" type="radio"/> None (N) <input type="radio"/> Required (R)	Availability (A) <input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)	

Para este ultimo pues es parecido al anterior aunque lo único que cambio es la dificultad ya que en este caso el Masquerading trata de hacerse pasar por un usuario, objetos u otras cosas que parecen ser legítimas o hasta seguras cuándo no es más que una máscara la cual está ocultando un software malicioso por detrás. Habiendo dicho lo que hay que hacer para conseguir que el ataque tanga un éxito, no creo que se algo sencillo pasar por la seguridad haciéndose pasar por otra persona o pasando un contenido, malicioso sin que sea detectado.

- Investigar en que consiste la denominada "Cyber Kill Chain", y cual es su aplicación en servicios de auditoría.

CKC es un proceso que se estableció por militares en su época la cual ahora se aplica al mundo tecnológico en el cual se categoriza por aumentar la seguridad de un sitio pero no de forma tradicional donde simplemente se aumentan las medidas de seguridad, sino que estudiando el ciclo de vida de un ataque. El ciclo de vida de un ataque se divide en 7 pasos los cuales se estudian para saber que hacer frente a un atacante ya que, al tratarse de una cadena, con que una parte se rompa o sale mal, las demás caen con ello donde además es más fácil aprender de ello para poder fortalecer las defensas frente a futuros ataques. Los siguientes pasos de un ataque en el CKC son los siguientes:

- Reconocimiento:
Esta parte es la primera la cual el atacante simplemente intenta recopilar todo tipo de información que sea a la vista, ya sea las medidas de seguridad que utiliza, como esta todo organizado mirando distintas redes sociales, por ejemplo. Con esto el atacante podrá ya pasar a la siguiente fase, pero para que esto no suceda lo mejor que se podría hacer es mantener muy controlado toda la información que sale limitando esta misma, ya sea en la página web oficial de la empresa o las redes sociales.
- Preparación:
Una vez que se tenga la información que se necesite, el atacante podrá empezar a desarrollar estrategias para poder realizar el ataque con más posibilidad de éxito y esto solo depende del apartado anterior donde como ejemplo: Digamos que los empleados de dicha empresa han dicho alguno que otro que está buscando nuevas ofertas de trabajo porque el suyo no les gusta del todo por X razón, por ende una forma fácil de realiza el ataque seria mediante phishing o si quizás en otro caso, la empresa está buscando perfiles nuevos para la empresa, si esta es descuidada perfectamente podría el atacante mandar un malware con el PDF mientras está suplantando la identidad de otro, como si estuviese usando Masquering (estos son solo ejemplo y entiendo que no sería tan fácil en ambos casos realizar dichos ataques).

- **Distribución**
Esta parte se vincula con los ejemplos que mencioné anteriormente donde ya se empieza a producir el ataque una vez que todo esté preparado y listo para la intrusión. En este caso es importante tener una seguridad elevada para entender qué tipo de ataque está sucediendo para prevenir dicho ataque.
- **Explotación**
Esta parte ya es la que empieza a ser crítica ya que es ejecutado el programa maligno en el cual se llegó a meter dentro de un sistema el cual pues ahora está infectado. En esta parte hay poco que los de sistema de seguridad puedan hacer acaso que sea localizarlo antes de que sea ejecutado el programa maligno. Es importante mencionar que esto puede llegar a explotar la vulnerabilidad encontrada por el atacante en la fase de preparación y que los ataques no tienen por qué comprometer a ordenadores, pueden ser varios los objetivos de los atacantes como los servidores o las distintas redes de una empresa.
- **Instalación:**
En esta parte no tiene porque el atacante instalar algo en la víctima, sino que podría ser un simple robo de credenciales como en el caso de Phishing, por ejemplo. Ya dentro, lo único que los equipos de ciberseguridad podrán hacer es monitorizar lo que está haciendo el atacante o intentar realizar alguna acción para forzar al atacante fuera del sistema a ser posible.
- **Comando y control**
Esta parte es en la cual ya nada se puede hacer, el atacante controla lo que quería y a través de la víctima estará realizando sus acciones maliciosas ya sea robo de dinero, credenciales, comprometer distintas partes de la compañía, llevarse documentación, o muchas otras más cosas.
- **Acciones sobre los objetivos**
Esta parte es ya la última donde el atacante intenta expandirse por toda la empresa o simplemente los objetivos que más interés tenga, y esta parte es sobre todo dar vuelta atrás, es decir volver a distribuir el programa maligno y seguir creciendo desde una manera aún más fácil ya que al llegar a esta parte el atacante tiene más control del cual tenía antes haciendo que toda esta cadena que he mencionado sea cíclica. Para romper la cadena se hace de dos formas, o se consigue parar al atacante o que este consiga lo que quería y decide terminar la cadena, por lo que es verdaderamente importante tener un sistema de seguridad muy avanzado, no solo como protección sino como respuesta a incidentes.
- Investigar al menos 2 casos de multas a una organización por incumplimiento de alguna de las leyes / normas vistas durante el presente tema. Podrán ser tanto de aplicación Española como extranjera.

Los ataques de los hackers no tienen por qué terminar cuando estos terminan, las empresas también tienen represalias del gobierno en el cual residen y dependiendo de lo grave de la situación pueden ser peores o mejores las multas que reciben las empresas de los ciber ataques, ya sea porque se ha robado mucha información personal de muchas personas, su dinero, u otras cosas de terceros. En estos casos sí que no es culpa de la empresa que les ataquen, pero sí que su culpa por no poderse haber defendido bien del ataque y por tener una seguridad tan baja para permitir esos ataques y estas son los dos ejemplos que elegí.

En Air Europa se realizó un ciber ataque en 2018 donde sufrieron una gran pérdida de datos de sus clientes y lo más importante de ese ataque fue que sobre todo se robaron los datos bancarios de estos mismos además de los personales. En esta situación la AEPD (Agencia Española de Protección de Datos) reaccionó a dicha situación con una multa de 600.000 euros y estos mismos analizaron los ataques y el sistema de seguridad de Air Europa donde estos decidieron que no eran suficiente las medidas de seguridad que tenían puestas. En total se llegaron a robar la información de 489.000 clientes aproximadamente de los cuales la empresa en cuestión notificó que se habían usado 4.000 tarjetas de crédito para cualquier cosa.

La otra noticia de la cual quería hablar ocurrió en Reino Unido donde la empresa Ticketmaster recibió como sanción, 1.5 millones de euros porque los atacantes consiguieron recopilar un total de 60.000 de tarjetas de crédito. Este ataque se consiguió gracias a una vulnerabilidad que residía en un chatbot el cual fue instalado por terceros y aun así, la ICO (Autoridad de Control Reino Unido) decidió que no se adecuaba el chatbot a la seguridad mínima que tenía que mantener una empresa como Ticketmaster y también estos no actuaron ni a tiempo ni adecuadamente ante dicha situación por lo que ICO tuvo que poner una sanción tan grande.

TEMA 4:

- Investigar como es posible cifrar una palabra con los algoritmos DES y AES mediante OpenSSL. Una vez hecho el alumno deberá comprobar el tiempo que se tardaría en descifrarlo mediante fuerza bruta con herramientas como Hashcat. Se deberá comparar la velocidad de ambos algoritmos, e indicar cuales han sido los comandos utilizados.

Para hacer uso de DES este codifica en grupos de 64 bits donde básicamente son 16 números hexadecimales y para encriptar este algoritmo usa claves las cuales también son grupos de 64 bits, aunque tiene una pequeña parte y es que cada octavo bit es ignorado, dejándolo en un total de 56 bits. Por otro lado, el AES coge en grupos de 128 y luego los cifra usando llaves de 128, 192 y 256 bits y para cifrarlo utiliza sustitución-permutación con múltiples rondas y estas mismas se definen como la cantidad de veces que se realiza la técnica de sustitución-permutación para terminar por cifrar el mensaje. Ahora como antes mencioné que hay 3 tipos de llaves que podemos usar, la de 128 bits lleva acabo 10 rondas, la de 192 bits 12 y por ultimo la de 256 bits lleva a cabo 14 rondas, pero por cada una de estas rondas se necesita una llave distinta por ronda las cuales todas parten de la primera.

Por desgracia en la demostración no podre enseñar mucho por varias razones:

- Por un lado, el hashcat ni otras herramientas me van bien en el ordenador, y no si ya es por mi ordenador, pero siempre me daba un mensaje de "Not enough space" o algo parecido en los demás programas.
- También cuando probaba hacer hasta una simple descriptación del hash de MD5 no me lo hacía siguiendo guías básicas dándome el mensaje de "Exahusted" sin descriptarme nada.
- Tuve que instalarme varias veces el hashcat y el Kali, ya que veía que no tenía los módulos que necesitaba para realizar la descriptación, al menos las instalaciones que descargaba.
- Por otro lado, al intentaba encriptas en DES con openssl me generaba un texto no leíble donde el hashcat no lo reconocía

Por otro lado me fije sobre todo en la encriptación AES, como explique anteriormente, dependiendo de los bits que se decida usar, habrá que hacer más rondas o menos para crear todas esas distintas claves

para cada ronda, pero ahora a la hora de pensar en ataques de fuerza bruta, me preguntaba cómo te efectivo sería, por un lado es obvio pensar que comparado al DES, se tardará muchísimo más en desencriptar algo que use el hash de AES.

Con las siguientes imágenes quiero demostrar los mensajes que me salían y a que me refiero:

```
(root@kali)~[/home/kali]
# ls
Desktop  Documents  Downloads  Music  Pictures  Public  target_hashes.txt  Templates  textoNormal.txt  Videos

(root@kali)~[/home/kali]
# openssl enc -des -in textoNormal.txt -out textoNormal.txt.enc
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

(root@kali)~[/home/kali]
# ls
Desktop  Downloads  Pictures  target_hashes.txt  textoNormal.txt  Videos
Documents  Music  Public  Templates  textoNormal.txt.enc

(root@kali)~[/home/kali]
# cat textoNormal.txt
mensaje oculto

(root@kali)~[/home/kali]
# cat textoNormal.txt.enc
Salted__UKzH%vBõ)

(root@kali)~[/home/kali]
#
```

Aquí podemos ver que estando en root, tengo creado un archivo de texto en el cual creándolo con touch y luego metiéndole un mensaje usando nano, lo encripto usando -des para decir que lo quiero encriptar en DES hash. Luego con el -in y -out son para decir que archivo es y donde quiero que resida el resultado de dicha encriptación donde luego con un cat miro el mensaje encriptado que como se puede ver esta el mensaje saltado y además aparecen esos caracteres ilegibles.

```
(root@kali)~[/home/kali]
# hashcat -a 3 -o descifrado.txt textoNormal.txt.enc
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-Intel(R) Core(TM) i5-9400H CPU @ 2.50GHz, 1422/1486 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashfile 'textoNormal.txt.enc' on line 1 (Salted__UKzH%vBõ): Token encoding exception
No hashes loaded.

Started: Sat Oct 9 16:46:13 2021
Stopped: Sat Oct 9 16:46:13 2021

(root@kali)~[/home/kali]
#
```

Luego después pues intenté usar hashcat donde el -a es para el modo que el 3 era para el ataque de fuerza bruta, -o para crear un fichero donde se guardará el resultado, y por ultimo el fichero que queremos que desencripte el programa, pero como era de esperarse, no entendió ningún hash y por ende lo dejó así.

- Investigar las diferentes técnicas de criptoanálisis para algoritmos simétricos.

Hay muchas distintas técnicas de criptoanálisis para algoritmos simétricos siendo dos de estos como los que vimos anteriormente (DES y AES) y donde voy a hablar de otras que no sean esas 2 ya que las mencioné anteriormente. Las que hablaré serán las siguientes:

- IDEA:
Este tipo de algoritmo tiene bastantes beneficios a la hora de cifrar, ya que, por un lado, permite hasta un peso de 2^{128} bits haciendo que se pueda guardar muchísimo más que en DEA Y AES juntas. Por otro lado, otras dos cosas por las cuales destaca es que todas sus operaciones son algebraicas y además al no haber operaciones en bits, hace que sea mucho más fácil a la hora de codificar
- BLOWFISH
De los que voy a mencionar este sería el más sencillo de usar donde las variables que usemos son seguras y permite utilizar claves entre 32 hasta 448 bits. Una de las desventajas que llegaría a tener es que es muy posible detectar algunas de las llaves que usa el algoritmo a las 14 rondas.
- TWOFISH
En términos de seguridad y eficiencia, supera al BLOWFISH con facilidad dejando que acepte las llaves de distintas longitudes y sigue un diseño sencillo para poder facilitar así el uso de su análisis y implementación. Por otro lado, a día de hoy no se ha encontrado ninguna vulnerabilidad así directa a lo que respecta el algoritmo, sí que se consigue con algún que otro ataque pero nada que sea así seguro que funciona siempre.
- Investigar en que consiste el 'salt' en un algoritmo simétrico, y como este puede aportar más seguridad al cifrado.

La manera más simple de explicar hacharle sal a un algoritmo simétrico es darle datos de manera aleatoria a un input de un hash para así conseguir un output también sea randomizado/único, aunque nos toquemos con el mismo input. Gracias a esto nos podemos proteger mucho mejor frente a los ataques de tipo vector mientras se ralentiza de los ataques de fuerza bruta, por ejemplo. Esto se debe a que cuando uno crea una contraseña usando el mismo tipo de hash, inevitablemente le saldrá el mismo output y esto pone en riesgo a muchas personas las cuales utilicen las mismas contraseñas, es decir si Pepe y Noelia usan “no12ca” como contraseña pues entonces les terminaría saliendo el mismo hash a los dos, pero por eso lo de la sal para que no sea así.

Por desgracia no podemos relajarnos con solo usar la sal ya que ataques a servicios online donde se tiene que poner las credenciales, uno puede usar un ataque de relleno de esos mismo y en algún momento le saldrá ya que los servidores en los cuales está la contraseña guardada ya le hecha sal al hashing.

- Investigar cuales son las principales técnicas de esteganografía utilizadas hoy en día y para qué son utilizadas en cada caso. Se deberá indicar el tipo de información que permite exfiltrar, y además el alumno deberá probar al menos una de las técnicas identificadas.

Para explicarlo de la manera ms simple, la esteganografía es usado en archivos de todos los tipos los cuales tendrán bits por ejemplo que no se usen y estos mismos serán reemplazados con otros bits que contengan todo tipo de información, aunque también podría ser que se aprovechando el tamaño de un archivo como un video se puede meter muchos datos entre medio . Para entenderlo más la principal diferencia entre esteganografía y criptografía es que en el primero intenta ocultar la existencia del mensaje en si mientras que el segundo intenta ocultar el contenido de mensaje. Ahora hablaré sobre los dos tipos de esteganografía que creo que son bastantes buenos y de una pequeña técnica de cada uno, por un lado, el de esteganografía de imagen y luego la de texto.

- Imagen, LSB (Least Significant Bit): Este funciona de una manera que explique anteriormente por encima donde lo que hace es coger los bits menos significativos de un archivo y los reemplaza con la información que quiere enmascarar. Lo bueno de este método es que se trata de algo simple además de que es efectivo pero su problema reside en su simpleza donde es muy vulnerable a cualquier análisis de cualquier tipo de análisis de esteganografía podría decodificar la información que tenga por detrás y para demostrara esto intentare esconder una imagen dentro de otra:

Image Steganography

[How it works](#)

[How to defeat it](#)

Hide images inside other images.

This is a client-side Javascript tool to steganographically hide images inside the lower "bits" of other images.

Select either "Hide image" or "Unhide image". Play with the **example** images (all 200x200 px) to get a feel for it.

Hide image

Unhide image

Cover image:

Seleccionar archivo

Ningún archi... seleccionado

Secret image:

Seleccionar archivo

Ningún archi... seleccionado

Hidden bits: 1

Example: Wikipedia Tree

Example: Walrus

Download Full-size Image



This is a project by [James Stanley](#).

Como podemos observar, lo que voy a hacer es esconder la imagen de la morsa en la de un árbol usando esteganografía por imágenes que es una forma de implementar el LSB ya que estoy metiendo la imagen de la morsa dentro de los bits de la imagen del árbol.

Image Steganography

[How it works](#)[How to defeat it](#)

Hide images inside other images.

This is a client-side Javascript tool to steganographically hide images inside the lower "bits" of other images.

Select either "Hide image" or "Unhide image". Play with the **example** images (all 200x200 px) to get a feel for it.

Hide image

Unhide image

Image:

Seleccionar archivo descarga.png

Example: N/A



Hidden bits: 1



Download Full-size Image



This is a project by [James Stanley](#).

Ahora como podemos observar voy a realizar el proceso inverso en el cual voy a desenmascarar la imagen y ver que contiene y efectivamente esta nuestra imagen de la morsa la cual como podemos ver no es que se vea 100% aun así.

- Texto, Format Based Method: Este tipo trata de esconder datos dentro de archivos de textos y esta técnica en específico lo que hace es alterar el formato del texto en concreto donde si se abre con un compresor de palabras, se notará la diferencia a lo largo del texto si se compara al original, donde no solo habrá espacios en blanco extra, sino que también que las letras de algunas palabras en si o tendrán distintos tamaños o hasta fuentes.

Bibliografía de los 4 temas (los enlaces van a la inversa, es decir los primeros enlaces son del tema 4 y así hasta el tema 1 que serán los últimos):

- S. James, (Sin fecha), Image Steganography, url: <https://incoherency.co.uk/image-steganography/#unhide>
- C. Archana, (Noviembre 2020), Steganography Tutorial – A Complete Guide For Beginners, url: <https://www.edureka.co/blog/steganography-tutorial#SteganographicTechniques>
- A. Monika, (Enero 2013), TEXT STEGANOGRAPHIC APPROACHES: A COMPARISON, url: <https://arxiv.org/ftp/arxiv/papers/1302/1302.2718.pdf>
- IEEE, (Abril 2014), An enhanced Least Significant Bit steganography method using midpoint circle approach, url: <https://ieeexplore.ieee.org/document/6949808>
- UKEssays, (November 2018), The Types and Techniques of Steganography, url: <https://www.ukessays.com/essays/computer-science/the-types-and-techniques-of-steganography-computer-science-essay.php>
- LA VANGUARDIA, (Febrero 2020), La esteganografía digital, la técnica que oculta información en archivos multimedia, url: <https://www.lavanguardia.com/vida/20200201/473240641630/la-esteganografia-digital-la-tecnica-que-oculta-informacion-en-archivos-multimedia.html>
- B. P. A. Alexis, H. H. D. Michelle, L. R. D. Edgardo, (Sin Fecha), Algoritmos Simétricos, url: <https://criptografia.webnode.es/algoritmos-simetricos/>
- Wikipedia, (Sin Fecha), Data Encryption Standard, url: https://es.wikipedia.org/wiki/Data_Encryption_Standard
- J. O. Grabbe, (Sin Fecha), The DES Algorithm Illustrated, url: <http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm>
- ClickSSL, (Junio 2021), Hashing vs Encryption – What are the Differences, url: <https://www.clickssl.net/blog/difference-between-hashing-vs-encryption>
- R. Pablo, (Marzo 2021), Unos ciberdelincuentes robaron los datos de miles de clientes de Air Europa en 2018; hoy la AEPD la multa por ello, url: <https://www.xataka.com/pro/unos-ciberdelincuentes-robaron-datos-miles-clientes-air-europa-2018-hoy-aepd-multa-ello>
- L. Zandilli, (Noviembre 2020), La ICO multa a Ticketmaster UK con 1,39 millones de euros tras un ciberataque a su chatbot, url: <https://aphaia.co.uk/es/2020/11/18/la-ico-multa-a-ticketmaster-uk-con-139-millones-de-euros-tras-un-ciberataque-a-su-chatbot/>
- ICO, (Noviembre 2020), ICO fines Ticketmaster UK Limited £1.25million for failing to protect customers’ payment details, url: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/ico-fines-ticketmaster-uk-limited-125million-for-failing-to-protect-customers-payment-details/>
- INCIBE, (Enero, 2020), Las 7 fases de un ciberataque. ¿Las conoces?, url: <https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces>
- MITRE ATT&ACK, (Sin fecha), ATT&CK Matrix for Enterprise, url: <https://attack.mitre.org>
- MITRE ATT&ACK, (Sin fecha), Phishing, url: <https://attack.mitre.org/techniques/T1566/>
- MITRE ATT&ACK, (Sin fecha), Exploit Public-Facing Application, url: <https://attack.mitre.org/techniques/T1190/>
- MITRE ATT&ACK, (Sin fecha), Abuse Elevation Control Mechanism, url: <https://attack.mitre.org/techniques/T1548/>
- MITRE ATT&ACK, (Sin fecha), Deploy Container, url: <https://attack.mitre.org/techniques/T1610/>
- MITRE ATT&ACK, (Sin fecha), Masquerading, url: <https://attack.mitre.org/techniques/T1036/>

- Scalefusion, (Sin Fecha), Mobile Device Management
- Software for a Modern Workforc, url: https://scalefusion.com/mobile-device-management?campaignid=882086140&adgroupid=47087471707&adid=431692288050&position=&utm_medium=ppc&utm_term=mobile%20device%20management&utm_source=ad-words&utm_campaign=Search-EU-MDM&hsa_kw=mobile%20device%20management&hsa_acc=6773144759&hsa_ad=431692288050&hsa_net=ad-words&hsa_src=g&hsa_tgt=kwd-135955665&hsa_grp=47087471707&hsa_mt=e&hsa_cam=882086140&hsa_ver=3&gclid=CjwKC-AjwkvWKBhB4EiwA-GHjFtXdZuCaDOLzhSYe-xVdZg1bSGpAdtPx_FKyfw85bHnLNiCi9Rt2gBhoC5cgQAvD_BwE
- Manage Engine, (Sin Fecha) Manage and secure devices, apps and data from a unified console, url: https://www.manageengine.com/mobile-device-management/?network=g&device=c&keyword=mdm&campaignid=10362720665&creative=463430444622&matchtype=p&adposition=&placement=&adgroup=104011326410&targetid=kwd-171730562&gclid=CjwKCAjw7--KBhAMEiwAxfpkWI0iSSfDxEcU9cn2XvX8NkmBAy5Xs5E80HevG6OVIPdN9UL8076xo-CBCAQAvD_BwE
- Gigatux, (Sin Fecha), 7.2 The Rule Sets, url: <http://books.gigatux.nl/mirror/snortids/0596006616/snortids-CHP-7-SECT-2.html>
- D. O. Daniel, (Marzo 2017), Qué es Snort: Primeros pasos, url: <https://openwebinars.net/blog/que-es-snort/>
- DragonJar, (Sin Fecha), PentBox - Una suite de seguridad y pentesting en ruby, url: <https://www.dragonjar.org/pentbox-una-suite-de-seguridad-y-pentesting-en-ruby.xhtml>
- Tensor, (Octubre 2014), Pent box security suite, url: <https://es.slideshare.net/Tensor/pent-box-security-suite>
- C. Akash, (Junio 2019), How To Install PentBox Tools On Kali Linux | Penetration Tool, url: <https://www.linkedin.com/pulse/how-install-pentbox-tools-kali-linux-penetration-tool-akash-chugh>
- W. Jack, (Octubre 2019), How to quickly deploy a honeypot with Kali Linux, url: <https://www.techrepublic.com/article/how-to-quickly-deploy-a-honeypot-with-kali-linux/>
- INCIBE, (Junio 2018), Honeypot, una herramienta para conocer al enemigo, url: <https://www.incibe-cert.es/blog/honeypot-herramienta-conocer-al-enemigo>
- R. Lukas, V. Johnny, H. Daniel, P. Andrea, CONPOT ,url: <http://conpot.org>
- Wikipedia, (Sin Fecha), NSA ANT catalog, url: https://en.wikipedia.org/wiki/NSA_ANT_catalog
- S. Der, (2013), NSA ANT catalog, url: https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf
- F. Yúbal, (Octubre 2019), Cómo funcionan los links de la Deep Web, url: <https://www.xataka.com/basics/como-funcionan-links-deep-web>
- G. V., (Noviembre 2020), Supuestos 'hackers' norcoreanos atacan a AstraZeneca, uno de los fabricantes de la vacuna contra la covid, url: <https://elpais.com/tecnologia/2020-11-27/supuestos-piratas-norcoeranos-atacan-a-astrazeneca-uno-de-los-fabricantes-de-la-vacuna-contra-la-covid.html>
- El Confidencial, (Agosto 2021), "Su cuenta quedará bloqueada": el nuevo fraude bancario vía SMS con el que acceden a tu cuenta, url: https://www.elconfidencial.com/tecnologia/2021-08-11/policia-alerta-fraude-bancario-sms-llamadas_3226540/

