

GUÍA TÉCNICA PRÁCTICAS INSTRUCTOR

MÓDULO 4. TALLER 7

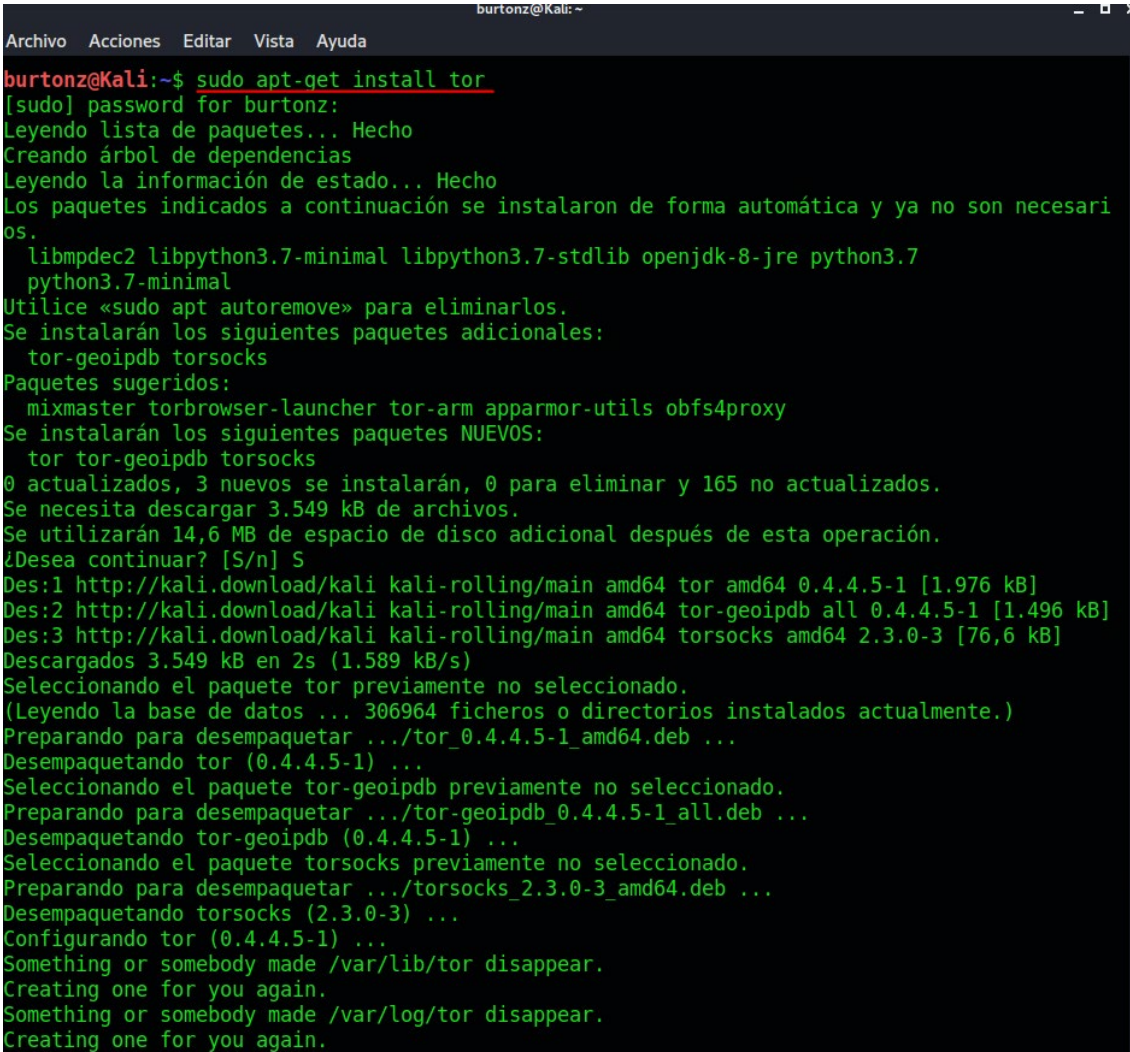
1. TALLER 7: BUSCANDO INFORMACIÓN EN LA DEEPWEB

Mediante una consulta usted deberá encontrar sitios donde pueda encontrar la adquisición de servicios de hacking en la Deep web. Ingresar a Kali Linux y desde Tor hacer la inspección correspondiente y como guía deberá usar la HiddenWiki: hiddenwiki7wiyzr.onion

Respuesta: Lo primero es encender la máquina Kali Linux y que tenga internet, se ejecutará Tor desde dicha máquina el cual ya viene configurado por defecto, así que usted debe seguir los siguientes pasos:

Paso 1: Instalar Tor en la máquina Kali Linux, esto es bastante sencillo, lo primero es insertar el siguiente comando dentro del terminal de Kali Linux: `sudo apt-get install tor`, ver Fig. 1.

Fig. 1. Instalando tor por consola

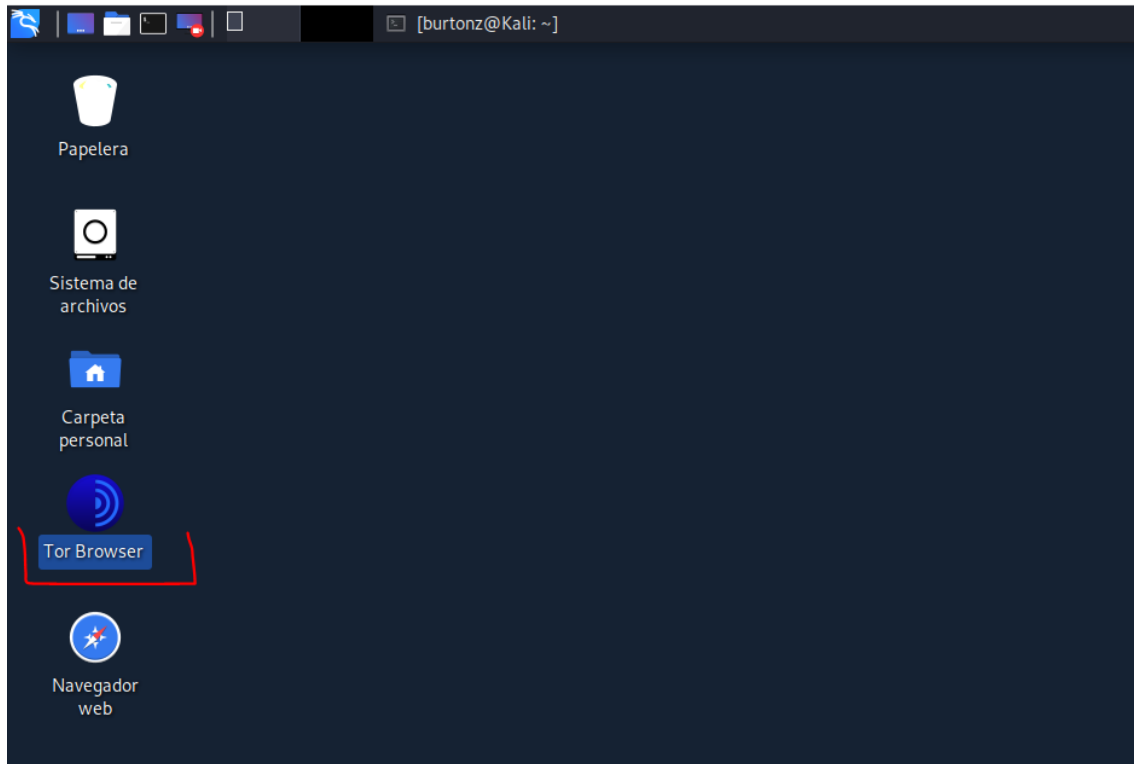


```
burtonz@Kali: ~  
Archivo Acciones Editar Vista Ayuda  
burtonz@Kali:~$ sudo apt-get install tor  
[sudo] password for burtonz:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesari  
os.  
  libmpdec2 libpython3.7-minimal libpython3.7-stdlib openjdk-8-jre python3.7  
  python3.7-minimal  
Utilice «sudo apt autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes adicionales:  
  tor-geoipdb torsocks  
Paquetes sugeridos:  
  mixmaster torbrowser-launcher tor-arm apparmor-utils obfs4proxy  
Se instalarán los siguientes paquetes NUEVOS:  
  tor tor-geoipdb torsocks  
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 165 no actualizados.  
Se necesita descargar 3.549 kB de archivos.  
Se utilizarán 14,6 MB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n] S  
Des:1 http://kali.download/kali kali-rolling/main amd64 tor amd64 0.4.4.5-1 [1.976 kB]  
Des:2 http://kali.download/kali kali-rolling/main amd64 tor-geoipdb all 0.4.4.5-1 [1.496 kB]  
Des:3 http://kali.download/kali kali-rolling/main amd64 torsocks amd64 2.3.0-3 [76,6 kB]  
Descargados 3.549 kB en 2s (1.589 kB/s)  
Seleccionando el paquete tor previamente no seleccionado.  
(Leyendo la base de datos ... 306964 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar .../tor_0.4.4.5-1_amd64.deb ...  
Desempaquetando tor (0.4.4.5-1) ...  
Seleccionando el paquete tor-geoipdb previamente no seleccionado.  
Preparando para desempaquetar .../tor-geoipdb_0.4.4.5-1_all.deb ...  
Desempaquetando tor-geoipdb (0.4.4.5-1) ...  
Seleccionando el paquete torsocks previamente no seleccionado.  
Preparando para desempaquetar .../torsocks_2.3.0-3_amd64.deb ...  
Desempaquetando torsocks (2.3.0-3) ...  
Configurando tor (0.4.4.5-1) ...  
Something or somebody made /var/lib/tor disappear.  
Creating one for you again.  
Something or somebody made /var/log/tor disappear.  
Creating one for you again.
```

Fuente: El autor

Paso 2: Una vez los instale busca el icono de tor navegador y le da doble clic sobre el para su posterior ejecución, ver Fig. 2.

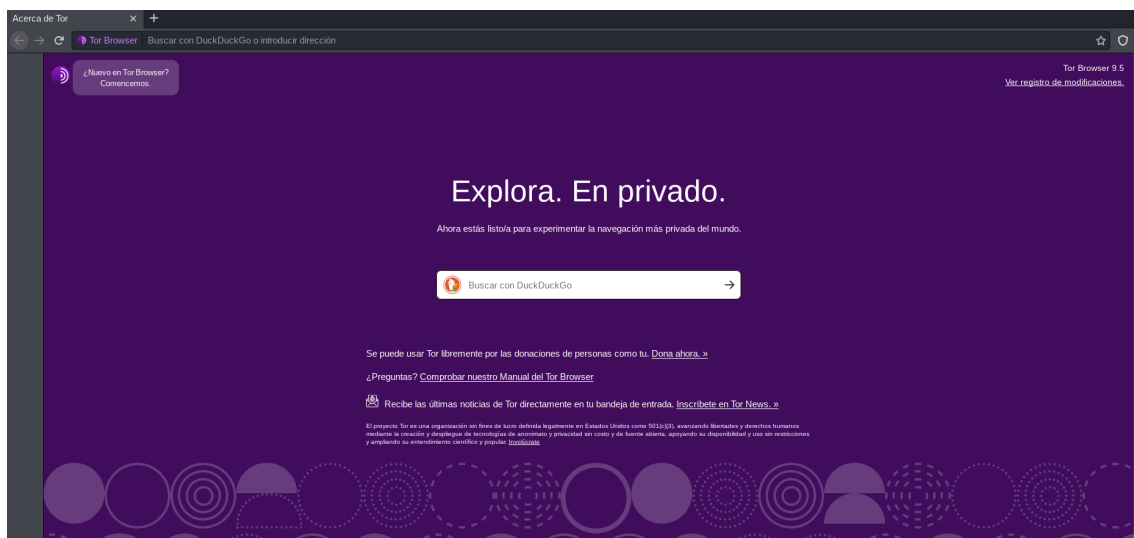
Fig. 2. Seleccionando navegador tor



Fuente: El autor

Paso 3: Dar doble clic sobre el navegador tor para su ejecución, ver Fig. 3.

Fig. 3. Ejecución navegador Tor

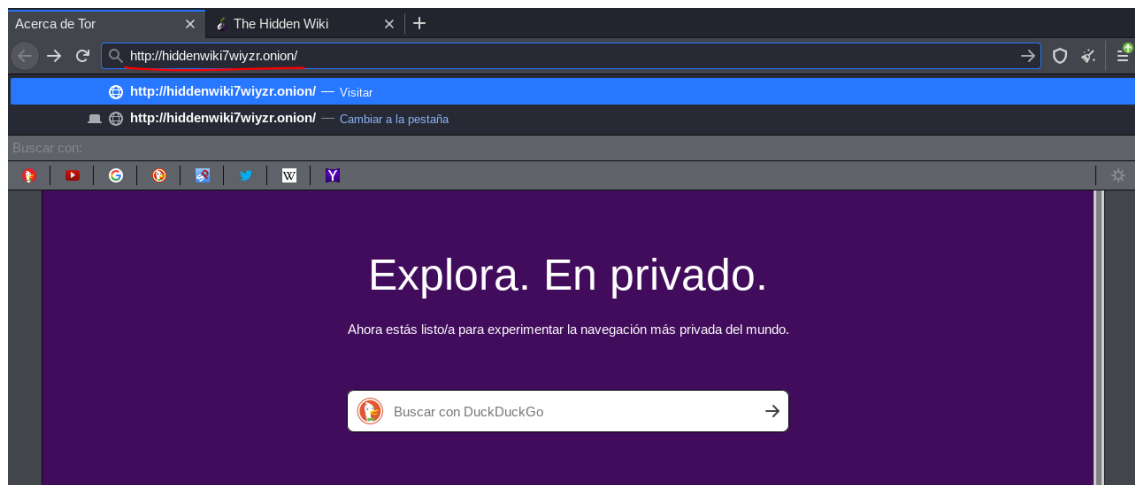


Fuente: El autor

Paso 4: Una vez dentro del navegador y según el enunciado de la actividad se debe hacer uso de la hiddenwiki que prácticamente es la guía oficial para navegar en

deepweb. En el navegador Tor se activa por defecto el buscador Duck Duck go, pero se deberá ingresar la dirección de la hiddenwiki en el navegador: hiddenwiki7wiyzr.onion ver Fig. 4.

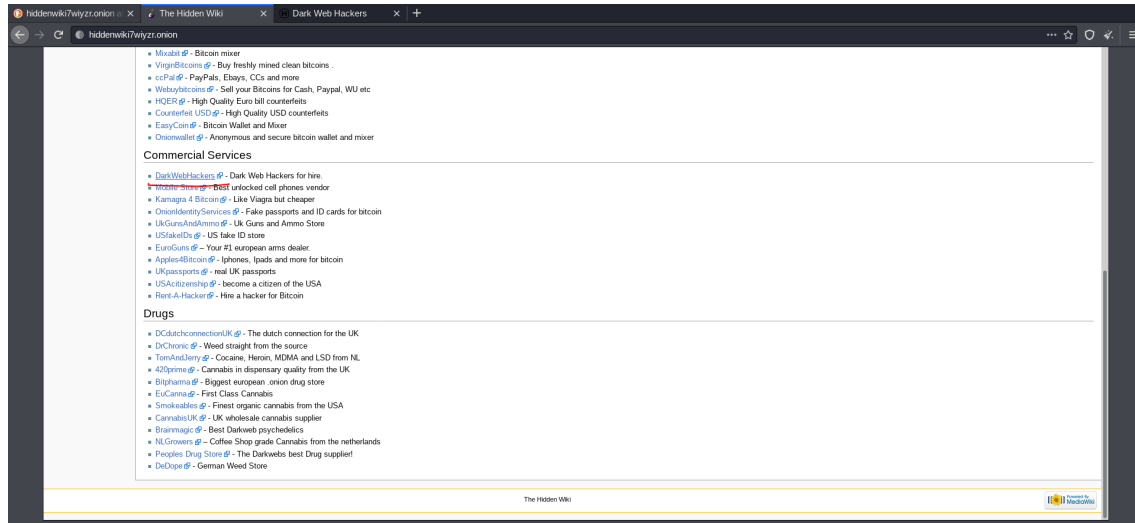
Fig. 4. Ingresando a la hiddenwiki



Fuente: El autor

Paso 5: Una vez en la hidden wiki se procede a buscar la sección de comercial services y allí se encontrará los servicios de un hacker que va desde escalada de privilegios hasta un DDoS, ver Fig. 5.

Fig. 5 Encontrando servicios de hacker en Deep web



Fuente: El autor

Paso 6: El último paso es poder ingresar a la página indicada en la hiddenwiki, hay que tener en cuenta que en los últimos meses los Gobiernos a nivel mundial le han dado de baja a muchos sitios de la deepweb los cuales pueden estar offline, para el ejemplo solicitado en el enunciado el sitio se encuentra funcionado, ver Fig. 6.

Fig. 6. Sitio de servicios de hacking

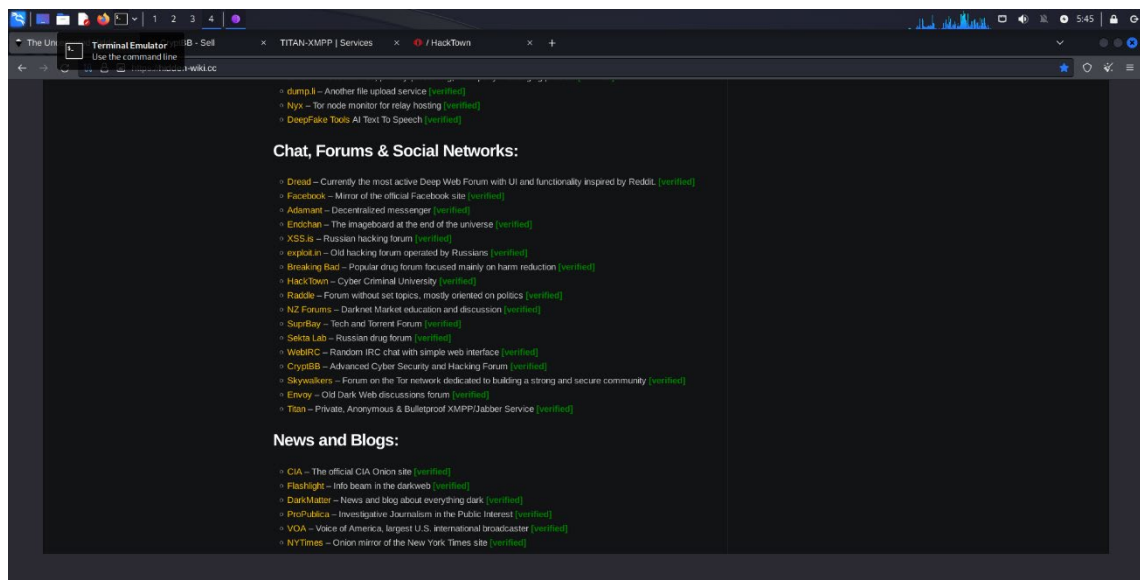


Fuente: El autor.

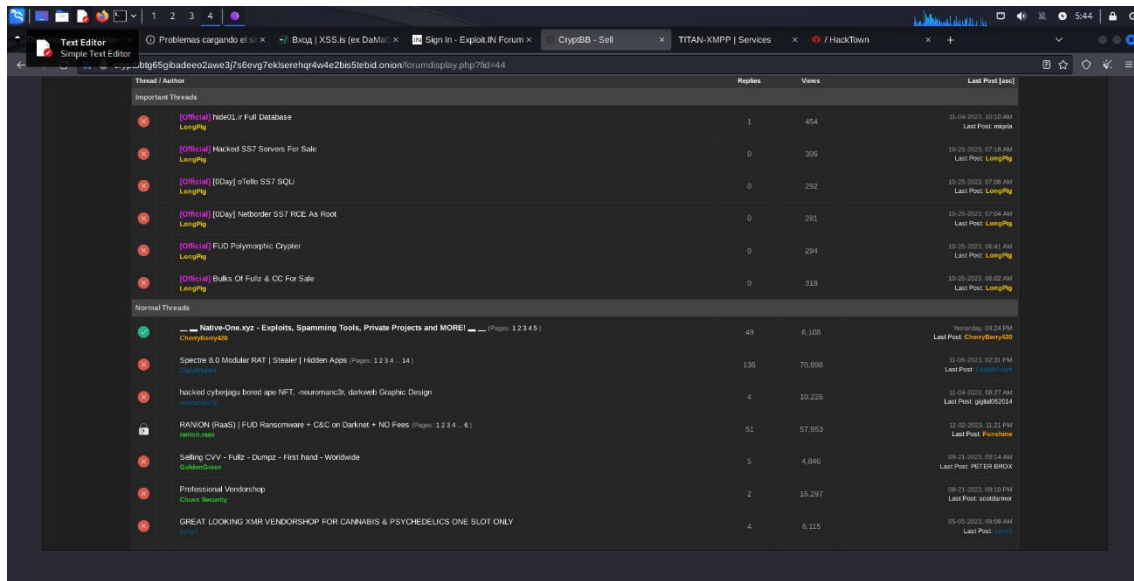
SOLUCIÓN.

Entrando en la página <https://hidden-wiki.cc/> en el navegador tor encontramos distintas categorías.

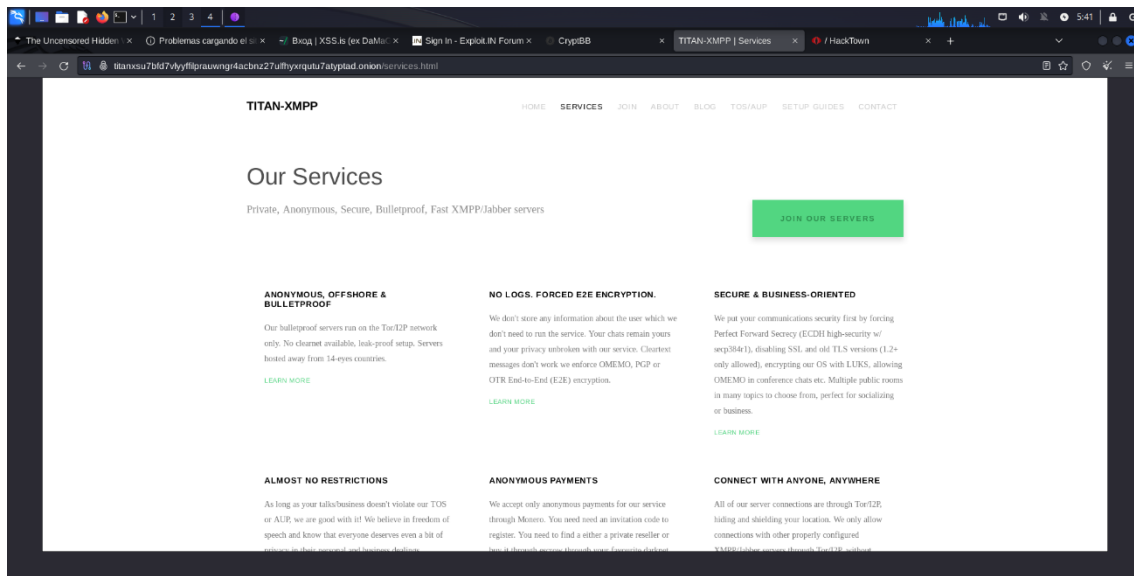
Entre ellas las de foros.



Entramos en los foros de hacking, algunas son de origen ruso y no puedo registrarme fácilmente.



Ofrecen servicios de malwares, carding, etc...



Firefox ESR
Browse the World Wide Web

Problemas cargando el...
Baq | XSS is (ex DaMac...
Sign in - English in Forum...
CrypIBB
TITAN-XPMP | Private Ar...
HackTown

2xavxcm23aocvzciakih3vek2ovzdggjvqd.onion/Members.php

Members

Forum	Topics	Posts	Last post by:
Updates and Information	8	8	June 2022 Updates Last post by Furshere

Hacking

Forum	Topics	Posts	Last post by:
ACT 0 - OPsec	3	233	Discussion and Support - 2022 Last post by Furshere
ACT I - Wi-Fi Hacking	3	701	Discussion and Support - 2022 Last post by Furshere
ACT II - Network and MITM attacks	3	113	Discussion and Support - 2022 Last post by Furshere
ACT III - Malicious Word Documents	3	273	Discussion and Support - 2022 Last post by Furshere
ACT IV - Scams and Tor Hidden Services	3	162	Discussion and Support - 2022 Last post by Furshere
ACT V - Phishflood	2	136	Discussion and Support - 2022 Last post by Furshere
ACT VI - Ride The Snake	2	120	Discussion and Support - 2022 Last post by Furshere
ACT VII - The Tale of a RAT	1	1	Discussions and Support - 2022 Last post by Furshere

Fraud

Forum	Topics	Posts	Last post by:
Credit Card Fraud	3	487	Discussion and Support - 2022 Last post by Furshere

The Armory

Forum	Topics	Posts	Last post by:
Cyber Arsenal Information	4	27	Native One Last post by Furshere

The Den

Forum	Topics	Posts	Last post by:
General Discussions	1	1	RULES Last post by Furshere
Cooperation	1	1	RULES Last post by Furshere

Question
Why is there a membership fee?

Answer:
Yes.