Escuela Colombiana de Ingeniería Julio Garavito

Diseño de Ambiente CTF para Entrenamiento en Ciberseguridad

Trabajo Dirigido

Daniel Ospina Bedoya

2019

Bogotá D.C

TABLA DE CONTENIDO

DESCRIPCIÓN DEL PROYECTO

OBJETIVO GENERAL

Diseñar un ambiente de aprendizaje de ciberseguridad centrado en competencias tipo CTF (Capture the Flag), mediante la identificación, desarrollo e implementación de un conjunto de herramientas y recursos tecnológicos y material de apoyo que permitan contar con un espacio que propicie el estudio y la investigación en el área.

OBJETIVOS ESPECÍFICOS

- Desplegar una plataforma de hosting y puntuación de competiciones tipo CTF.
- Investigar y aplicar estándares y procedimientos usados en competencias internacionales de solución de CTFs u otras competencias de seguridad.
- Producir un índice de información para la investigación y aprendizaje sobre el desarrollo y solución de retos CTF.

ENTREGABLES

- Plataforma funcional para hosting y calificación de retos CTF. Con su respectiva documentación
- Recopilación de información sobre competencias y estándares CTF y relacionados como base de conocimiento para el área de seguridad en la decanatura.
- CTFs diseñados para prácticas, acompañados por material de apoyo relacionado
- Artículo de investigación sobre el tema del proyecto sometido a revista tipo B o C según el sistema de indexación de Colciencias.

JUSTIFICACIÓN

Las competencias de seguridad informática cada vez toman más fuerza alrededor del mundo, y han probado ser herramientas muy efectivas para el aprendizaje de conceptos de seguridad e informática, así como un ambiente de práctica controlado y seguro para estudiantes y profesionales del área IT. Generar una infraestructura para apoyar la generación de conocimiento durante las asignaturas y eventos que se llevan a cabo en la decanatura es de gran valor para ésta.

METODOLOGÍA PROPUESTA

El desarrollo del proyecto tendrá la siguiente estructura para completar los objetivos específicos.

I. Investigación de posibles plataformas para hosting, y puntuación de CTFs.

   Obtener una comparativa de las opciones disponibles, y el proceso llevado para la elección de la plataforma a usar en el semillero.

II. Montar y configurar el servidor.

   Documentar el proceso de instalación y configuración de la plataforma.

III. Investigación y recopilación de categorías y retos.

   Generar una base de conocimiento con marco teórico, retos y solución de CTFs.

IV. Valor agregado

   Documentación y tecnología adicional relacionada con el proyecto, así como trabajo futuro disponible para el desarrollo del semillero.

MARCO TEÓRICO

¿QUÉ ES UN CTF?

CTF (Capture The Flag) es un tipo de competencia de seguridad informática que desafía a los concursantes a resolver una variedad de tareas que van desde una búsqueda de un dato específico en wikipedia, ejercicios básicos de programación, hasta hackear un servidor para robar datos. En estos desafíos, generalmente se le pide al concursante que encuentre un texto específico que pueda estar oculto en el servidor o detrás de una página web. Este objetivo se llama la bandera, de ahí el nombre [1].

Las competencias de Capture the Flag (CTF) son los eventos más populares en las conferencias de ciberseguridad donde los participantes pueden demostrar sus habilidades. Además, el CTF es ampliamente reconocido como una valiosa herramienta pedagógica para proporcionar a los estudiantes problemas de la vida real en el área de seguridad informática; donde se desarrollan habilidades como trabajo en equipo, aprendizaje activo y colaborativo basado en retos, entre otras [2].

TIPOS DE CTF [3]

Ataque

En este tipo de CTF los equipos compiten completando únicamente tareas ofensivas, donde el organizador provee la infraestructura para los servicios vulnerables. Cada bandera otorga un número definido de puntos, las cuales se obtienen al explotar exitosamente un servicio o completando un enigma o acertijo. El estilo más popular de CTF de sólo ataque es “Jeopardy” donde los retos se clasifican por dificultad y categoría, como esteganografía, criptografía, web, forensia, etc. Este tipo de CTF escala bien a eventos con gran número de equipos.

Defensa

En este tipo de CTF los equipos participantes tienen la tarea de asegurar servicios vulnerables ya desplegados, junto con tareas de “negocio” adicionales cumpliendo ciertos requerimientos establecidos. Donde solo un equipo coordinado por el organizador actúa como equipo rojo “Red Team” con tareas ofensivas. Usualmente la calificación es manual, y los criterios de evaluación cambian según evento.

Ataque-Defensa

Este tipo de CTF se caracteriza dado que los equipos tienen la tarea de asegurar servicios vulnerables y atacar servicios equivalentes de otros equipos. Puntos son otorgados por mantener servicios funcionando el mayor tiempo posible y reducir el número de vulnerabilidades presentes; así como obtener las banderas de equipos contrarios.

WarGames

No debe confundirse un CTF con un WarGame; aunque similares los WarGames son una serie retos que no están limitados por tiempo, y estos no requieren la organización de un evento para su desarrollo, cumplen una función netamente de aprendizaje y entretenimiento.

Competencias de seguridad tipo CTF

DEF CON

Sin duda alguna la Competición (y conferencia de hacking) más grande y prestigiosa del mundo, se celebra en Las Vegas cada agosto y tiene una ronda de clasificación previa al evento.

PicoCTF

Una de las competencias CTF más reconocidas, en donde pueden participar estudiantes de secundaria y preparatoria, organizada por la Universidad Carnegie Mellon.

Pwn2Own

Se realiza anualmente en la conferencia CanSecWest, con premios de alrededor de $100.000 dólares. Esta conferencia contiene una sub-competencia organizada por Google en búsqueda de vulnerabilidades en Chrome OS.

Otras Competiciones

Otras competencias reconocidas son:

- NCCDC: National Collegiate Cyber Defense Competition
- Mitre Cyber Academy
- National Cyber League

Puntuación y calificación de CTFs

Cada evento tiene su propio sistema de calificación, que depende del tipo de CTF que se esté realizando. Puntuación automática generalmente se controla en una plataforma donde cada equipo sube la bandera que ha encontrado; esta bandera puede ser estática o una expresión regular. Donde cada bandera otorga un puntaje determinado, y este puntaje puede ir decayendo según el orden y número de soluciones, según lo estimado por los organizadores. La puntuación automática es común en CTFs de solo ataque.

Para CTFs de Ataque-Defensa, los equipos suman puntos por mantener los servicios funcionando el mayor tiempo posible, donde un sistema hace peticiones al servicio periódicamente para comprobar su estado. En este tipo de CTFs es muy importante el balance

de la puntuación de defensa y ataque, donde equipos que se desempeñan bien en ambas áreas son recompensados, de esta forma se evalúa el mejor equipo y la competencia se mantiene interesante [3].

Los CTF tipo Defensa requieren que el equipo ofensivo de la organización monitoree constantemente el estado de los servicios, y manualmente puntuar según el rendimiento de cada equipo, dado que sistemas automáticos requieren tener en cuenta demasiados escenarios y casos de frontera. Es por esto por lo que este tipo de competencias se hacen a menor escala, y un número reducido de equipos.

CATEGORÍAS DE RETOS CTF

Entre las categorías de retos más comunes en estas competencias se encuentran:

1) Ingeniería Inversa

La ingeniería inversa es el proceso de tomar una salida y descubrir cuál era la entrada. También significa rastrear los pasos que tomó una pieza de información desde que se ingresó hasta que se emite. Usualmente requiere la depuración del código para seguir los pasos y organizarlo para que este tenga un significado y extraer la información necesaria [4].

2) Explotación Binaria

La explotación binaria es el proceso de abusar de defectos sutiles (o quizás no tan sutiles) en el software para hacer que una aplicación realice funciones que no estaba diseñada para realizar.

3) Criptografía

Los retos de criptografía requieren el estudio, uso o explotación de algoritmos criptográficos para extraer información. El participante se apoya de herramientas criptográficas y su capacidad de analizar información encriptada para encontrar pistas para la solución del problema.

4) Forense

Los retos forenses buscan que el participante a partir de evidencia digital forense como logs, capturas de tráfico, volcados de memoria, etc. Extraiga información a partir de métodos forenses para obtener la bandera.

5) Redes

Los retos de redes se basan en el conocimiento y utilización de herramientas y software de infraestructura tecnológica, el conocimiento de protocolos y el análisis de datos, donde a partir de estos puede extraer la bandera.

6) Esteganografía

Este tipo de reto requiere que los participantes separen información en archivos que contienen datos ocultos mediante técnicas esteganográficas.

7) Web

Los retos tipo web es una de las categorías más populares en CTFs, la cual trata de explotar o aprovechar falencias en aplicaciones web, su programación o las tecnologías con las que fueron creados; extrayendo así la bandera.

8) Trivia/Otros

Los retos tipo trivia buscan desafiar el conocimiento conceptual de los participantes en diferentes temáticas, los participantes reciben preguntas de un tema específico donde la respuesta es la bandera.

PLATAFORMA CTF

ELECCIÓN DE LA PLATAFORMA

Entre las plataformas más usadas para realizar competiciones CTF, se generó una lista para analizar la más adecuada para nuestras necesidades:

Dirección del recurso en github.com/

- CTFd/CTFd
- facebook/fbctf
- google/ctfscoreboard
- picoCTF/picoCTF
- mcpa-stlouis/hack-the-arch
- Nakiami/mellivora
- UnreaalAkama/NightShade
- easyctf/librectf
- koromodako/mkctf
- moloch--/RootTheBox
- legitbs/scorebot

El primer filtro generado para escoger la plataforma se basó en una investigación de casos de uso, popularidad, documentación y fecha de última actualización, en búsqueda de sacar de la lista plataforma con pobre documentación y con pocas características o mantenibilidad.

Se eligieron entonces cuatro plataformas, las cuales se montaron sobre máquinas virtuales, se probaron y analizaron las características. Se evaluó su facilidad de uso, configuración y mantenibilidad. Y como criterios finales el lenguaje de programación, así como algunos comentarios subjetivos se tuvieron en cuenta. Un resumen de este proceso se compiló en una hoja de cálculo, adjunta a este documento.

	Scoring	Individual	Teams	Registration	Automatic Start & End	Import & Export CTF Data	Challenge File Upload	Frontpage News & Announcements	Hints	Plugins	SMTP Support	Chat	Graphs & Stats	Language	Programming Language
CTFd	yes	yes	yes	Self and Admin | Admin Toggle	yes	yes	Multiple	yes	yes	yes	yes	no	High Quality	English	Python
FBCTF	yes	No*	yes	Self or Tokenized | Admin Toggle	yes	yes	No	yes	yes	no	no	no	no	Multi	PHP
HackTheArch	yes	No*	yes	Self Only | Admin Toggle	yes	No	No	Frontpage Only	yes	no	yes	yes	Simple	English	Ruby
Mellivora	yes	No*	yes*	Self Only | Always Public	yes	no	Multiple	yes	yes*	no	yes	no	no	English	PHP

Como resultado final, se eligió CTFd, dada su reputación, constante actualización, alta documentación, y facilidad de uso. También por el lenguaje de programación usado, python, que se enseña en tanto en la facultad de ingeniería de sistemas de la escuela, como en toda la universidad.

INTRODUCCIÓN A CTFD

¿Qué es CTFd?

CTFd es un marco de Capture The Flag que se centra en la facilidad de uso y la personalización. Viene con todo lo que necesita para ejecutar un CTF y es fácil de personalizar con complementos y temas [5].

Características

- Cree sus propios desafíos, categorías, pistas y banderas desde la interfaz de administración
    - Desafíos de puntuación dinámica
    - Desafíos desbloqueables
    - Creación de desafíos personalizados mediante arquitectura de complementos para retos.
    - Banderas estáticas y basadas en expresiones regulares
        - Complementos personalizados para banderas
    - Pistas desbloqueables
    - Subida de archivos al servidor o a un back-end compatible con Amazon S3
    - Limitación de intentos y ocultar los desafíos
    - Protección automática de intentos por fuerza bruta
- Competiciones individuales y por equipos.
    - Los usuarios pueden jugar solos o formar equipos.
- Cuadro de indicadores con resolución de empate automática
    - Ocultar puntuaciones públicas
    - Congelar puntajes en un momento específico
- Gráficos comparativos de los 10 mejores equipos y gráficos de progreso de equipos
- Sistema de gestión de contenidos usando Markdown
- Soporte de correo electrónico SMTP + Mailgun
    - Soporte de confirmación por correo electrónico
    - Olvidé mi contraseña
- Inicio y finalización automática de la competencia.
- Gestión de equipo, ocultamiento y suspensiones.
- Personalice todo mediante interfaces de plugins y temas
- Importación y exportación de datos CTF
- Y mucho más...

INSTALACIÓN Y CONFIGURACIÓN DE CTFD

Consideraciones Previas

Los siguientes pasos para la instalación son realizados sobre una instalación mínima[1] de la distribución Slackware. La instalación asegura el funcionamiento sobre Slackware 14.2, y los paquetes presentes en el disco de instalación en esta versión. Así como el software al momento de la realización de este documento[2]. Dado que este software se encuentra bajo constante desarrollo, no se asegura la consistencia de esta guía; esto no implica (ni se recomienda) realizar futuras instalaciones bajo la misma versión, sino seguir la documentación oficial en caso de que esta guía no contemple alguna actualización. La documentación oficial de instalación está disponible en: https://github.com/CTFd/CTFd/wiki/Advanced-Deployment

Pasos para la Instalación

1. Previo a la instalación se requiere la instalación de las siguientes dependencias o paquetes, estos están disponibles en el disco de Slackware 14.2 y/o en la web https://slackware.pkgs.org/14.2/slackware-x86_64/ :
   - git
   - gcc
   - python-dev
   - python-pip
   - python-setuptools
   - libffi-dev
   - mysql (mariadb)
   - libaio-0.3.109
   - jemalloc-3.6.0
   - which-2.21
   - tcl-8.6.5
   - tk-8.6.5
2. Se debe completar la instalación y correr los scripts para asegurar la base de datos, la documentación oficial de slackware contiene los pasos a realizar. https://docs.slackware.com/howtos:databases:install_mysql_on_slackware

3. Instalación de Redis
   Se obtiene la última versión estable de redis:

   ```
   wget http://download.redis.io/redis-stable.tar.gz
   ```

   Se descomprime el archivo, y nos movemos a la carpeta correspondiente

[1] Instalación con los paquetes mínimos para el funcionamiento de Linux Slackware.

[2] 17-Sept-2019 bajo el último commit a la fecha en el repositorio oficial en github: https://github.com/CTFd/CTFd/tree/b8c1970b8e82ef1d82377d763980d934eca6727f

```
tar xvzf redis-stable.tar.gz

cd redis-stable
```

Iniciamos la instalación estándar con make

```
make
```

Comprobamos que el build funciona correctamente mediante, si este falla, el software no funcionará correctamente al final de la instalación, es necesario mirar los logs para solucionar problemas de dependencias o conflictos.

```
make test
```

Finalizamos la instalación mediante

```
make install
```

Copiamos el archivo de configuración por defecto

```
cp redis.conf /etc/redis.conf
```

Editamos el archivo, agregando una contraseña (mínimo 32 caracteres aleatorios[3]), buscando la línea `# requirepass foobared` se quita el comentario, y se cambia "foobared" por una contraseña segura.

Le indicamos a rc.local que el servicio redis se debe iniciar al iniciar la máquina. Agregando las siguientes líneas a rc.local.

```
# Start Redis Server Daemon

/usr/local/bin/redis-server /etc/redis.conf --daemonize yes
```

4. Actualizar PIP

```
pip install --upgrade pip
```

5. Se clona el repositorio oficial de CTFd en la carpeta /usr/local/

```
git clone https://github.com/CTFd/CTFd
```

6. Se cambia a la carpeta de CTFd

```
cd CTFd/
```

[3] Dado que redis es un servicio pensado para responder peticiones en grandes volúmenes, un atacante puede probar hasta 150.000 contraseñas por segundo (según la documentación de de redis), por lo tanto se vuelve muy importante tener una contraseña segura.

7. Se instalan los requerimientos vía pip

```
pip install -r requirements.txt
```

8. Se edita el archivo /CTFd/CTFd/config.py, según las indicaciones propuestas en https://github.com/CTFd/CTFd/wiki/Advanced-Deployment

    a. URL de la base de datos:

```
mysql+pymysql://root:[<password>]#@localhost/ctfd
```

    b. URL del servidor Redis:

```
redis://:[<contraseña-redis>]@localhost:6379
```

    c. Llave de seguridad:

```
SECRET-KEY [String aleatoria de 32 caracteres]
```

9. Se crea un directorio para guardar los logs:

```
mkdir /var/log/CTFd
```

10. Se instala el HTTP server “gunicorn” mediante:

```
pip install gunicorn
```

11. Se agrega las siguientes líneas a rc.local para iniciar CTFd al momento de iniciar la máquina (y con el mismo comando se puede iniciar manualmente el servidor)

```
# Start CTFd using gunicorn

      gunicorn --chdir /usr/local/CTFd --bind 0.0.0.0:80 -w 5 --
      worker-class gevent "CTFd:create_app()" --access-logfile
      "/var/log/CTFd/access.log" --error-logfile
      "/var/log/CTFd/error.log" --daemon
```

CONSIDERACIONES ADICIONALES DE CTFD

DNS

El servidor CTFd se encuentra en la infraestructura del laboratorio de informática, bajo el nombre: obsidiana.is.escuelaing.edu.co

Proceso de Actualización de CTFd

Dado que la instalación de CTFd proviene completamente de GitHub y no existen releases oficiales, las actualizaciones se realizan a través de git, para esto:

1. Se debe confirmar que el repositorio remoto apunta al repositorio oficial de CTFd: "https://github.com/CTFd/CTFd.git" para esto se utiliza el comando:

   ```
   git remote show origin
   ```

2. Mediante "git status" se debe confirmar que los únicos archivos con cambios presentes en el repositorio local son: ./CTFd/config.py y ./CTFd/dump.rbd

   El primero es el archivo de configuración que se trabaja durante la instalación, y el segundo es un archivo de persistencia de redis. Como estos dos archivos usualmente no son actualizados por los desarrolladores, para actualizar solo es necesario correr el comando: "git pull origin master".

   Si por algún motivo este comando falla dado a un problema de conflictos, se debe revisar con cuidado que hace cada archivo y que los conflictos no sean archivos de configuración o producción y puedan afectar el servicio como se encuentra en ese momento. Dependiendo de la situación se debe tomar la decisión de hacer una reinstalación completa de la plataforma, o hacer un commit de los cambios, (si aplica) arreglar conflictos, y posteriormente reintentar el pull.

SELECCIÓN DE RETOS

El objetivo con el repositorio de retos es tener una serie de retos frecuentes, modificables y complementarios a el aprendizaje en asignaturas del área de seguridad e infraestructura. Cada reto contiene indicaciones para su preparación, solución y bibliografías. De esta forma es posible para los profesores establecer actividades académicas a partir de este repositorio y la plataforma CTFd.

PROCEDIMIENTO

Para la selección de retos se realizó a partir de soluciones o como comúnmente se conocen "writeups" de retos de CTFs realizados alrededor del mundo. Estos writeups usualmente son publicados por los participantes de los eventos en sitios web o plataformas como GitHub; aunque también es posible encontrar writeups publicados por los organizadores de los eventos, principalmente para retos que no fueron solucionados el día del evento.

El mayor inconveniente al momento de reunir retos es la falta de código fuente de retos que no se solucionan completamente en equipos de los participantes, estos recaen principalmente en las categorías Web y Networking. En estos casos es usualmente necesario generar por sí mismo el código fuente de estos retos y realizar las pruebas correspondientes. No hay una forma específica más eficiente para encontrar retos, los mejores resultados se obtuvieron a partir de la búsqueda de términos como "writeup" o "CTF" en plataformas como GitHub. A partir de aquí es encontrar repositorios con writeups que expliquen bien la solución para realizar un trabajo inverso para la generación del código fuente o casos bases para el reto.

CATEGORÍAS, DIFICULTAD Y MODIFICACIÓN DE RETOS

En categorías como esteganografía o criptografía, se encuentra fácilmente los archivos que se distribuyen a los participantes, aunque igualmente se construyó una guía para personalizar el reto y la bandera de estos retos.

Los retos del repositorio se encuentran ordenados de la siguiente forma:

- Retos por Categoría
    - Reto por Dificultad

La dificultad se indica por un tag (Ej: [M]) antes del nombre, donde:

- [E] = Easy
- [M] = Medium
- [H] = Hard

Estas dificultades son estimadas frente a los conocimientos que se adquieren en la materia Seguridad Informática o Seguridad y Privacidad de TI, es un estimado vago y debe ser tomado ligeramente.

Estos retos se organizaron de tal manera para facilitar tanto como fue posible su modificación y organización, se recomienda a organizadores modificar los retos (títulos, contenido y banderas) para minimizar probabilidades de fraude o búsqueda de solución en internet.

Adicionalmente el repositorio contiene README.md que detallan y organizan varios aspectos del repositorio; así como un plantilla.md como base para la creación de nuevos retos.

RETOS PRESENTADOS

Como parte de la serie inicial de retos, se agregan al repositorio como primera versión presentada a la entrega del proyecto, los siguientes retos:

- Cryptography
    - [E] File Recovery
    - [E] Some martian message
    - [H] XORnigma
    - [M] Alphabet
    - [M] Shiny
- Forensics
    - [E] Hey Chuck where is the flag
    - [H] Someone steal my flag
    - [M] Easy Trade
- Networking
    - [E] HIDDEN
    - [E] is this an IP
    - [H] Repeat please
    - [M] Wake me up
    - [M] Who I am
- Other
    - [E] Social
    - [M] Old School
- Reverse-Binary
    - [E] ASSEMBLY
    - [M] 1996
    - [M] I love this guy
- Steganographyç
    - [E] I love images
    - [E] Multiple flags
    - [H] Try to see mee
    - [M] A ghost sound

    - [M] Hack a nice day
- Web
    - [E] God of gamble
    - [H] My admin panel
    - [M] Not(e) Accesible
    - [M] flags

Los retos presentados son una combinación de retos tomados desde writeups, generados autónomamente a través del proyecto y una combinación de ambos. Toda la documentación de cada reto, así como organización y referencias se encuentra en el README.md de cada reto.

MODIFICACIÓN DE REPOSITORIO

Este repositorio se anexa como resultado del proyecto y tiene dos copias remotas: una en la plataforma GitLab de Labinfo y otra en GitHub. Ambos son repositorios privados, puesto que el repositorio está enfocado en usuarios administradores como profesores que busquen aplicar retos en sus clases u organizar un CTF.

Para acceder al repositorio interno de labinfo, contactar a la administración del laboratorio de informática. El administrador debe agregar su usuario de LabinfoGitlab como integrante del grupo CEATyS para así de esta forma ser colaborador del repositorio de RetosCEATyS.

El repositorio público https://github.com/danielospina-b/RetosCTF-CEATyS es una copia del repositorio interno de labinfo, y tiene por objetivo ser un backup en caso de cambios sobre la plataforma del laboratorio por lo tanto cambios realizados al interno sería ideal moverlos también a este repositorio; para esto escribir a: daniel.ospina-b@mail.escuelaing.edu.co para solicitar acceso.

REFERENCIAS

[1] atan, «What is CTF and how to get started!,» 28 Marzo 2019. [En línea]. Available: https://dev.to/atan/what-is-ctf-and-how-to-get-started-3f04. [Último acceso: 15 Diciembre 2019].

[2] A. Mansurov, «A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia,» 17 Agosto 2016.

[3] A. Davis, T. Leek, M. Zhivich, K. Gwinnup y W. Leonard, «The Fun and Future of CTF,» Julio 2014.

[4] OJ., «Difference Between Binary Exploitation and Reverse Engineering?,» 26 Enero 2014. [En línea]. Available: https://security.stackexchange.com/questions/49320/difference-between-binary-exploitation-and-reverse-engineering. [Último acceso: 16 Diciembre 2019].

[5] CTFd Developer Team, «CTFd,» [En línea]. Available: https://github.com/CTFd/CTFd. [Último acceso: 19 Noviembre 2019].