# Desarrollo de rutinas que resuelvan vulnerabilidades detectadas por la utilización de herramientas de hacking ethical

**Tópico de evento:** ciberseguridad.

**Autor:** Brayan Sánchez Torres.

Estudiante de ingeniería de sistemas.

**Semillero de investigación:** SIGLAS.

**Grupo de investigación:** INGAP.

Universidad Francisco de Paula Santander Ocaña.

**Email:** bsanchezt@ufpso.edu.co

Telefono: 3168354450.

**Keywords:** Scripts, Hacking ethical, Front-end.

Introducción:

Actualmente el uso del software por parte de los usuarios solo se basa en el FRONT-END, debido a esto la mayoría de las personas solo conocen el propósito del software más no el funcionamiento del mismo, por tal razón los usuarios son vulnerables a recibir ataques por cosas tan simples como una mala configuración. Cabe resaltar que no todas las personas deben tener conocimientos profundos en el desarrollo de software pero en un mundo de constante cambio tecnológico y la relación estrecha que se ha hecho entre las personas y la tecnología se debe generar una cultura de conocimiento informático general que abarque conocimientos base sobre software y las tecnologías existentes.

El desarrollo de rutinas (scripts) se basa en cubrir una vulnerabilidad que es detectada con tecnologías de hacking ethical, además de encontrar algunas necesidades, pero para lograr esto se debe tener conocimientos base de los sistemas a trabajar aquí es donde se entra a generar conocimientos bases en cuanto estos sistemas, obteniendo la vulnerabilidad a trabajar se desarrolla una rutina en lenguaje Python debido a que este tiene una buena curva de aprendizaje y la vez es bastante potente.

El objetivo principal de la propuesta es dar a conocer pautas o metodologías que se entregarán junto con software que utilizado de la manera que se expresan en las metodologías, harán que la persona encuentre sus propias vulnerabilidades o problemas, y sea capaz de resolverlas a través del desarrollo de scripts.

Uno de los puntos fuertes de la propuesta es que se quiere infundir una cultura de interés por el conocimiento referente al mundo de las tecnologías informáticas y de autosuficiencia en cuanto a problemas relacionados con el software pero con un grado complejidad por mucho mediano ya que no siempre las cosas se podrían resolver con scripts y esto llevaría a desarrollo de software potente por lo cual sería demasiado complejo.

Objetivo general:

Resolver problemas de vulnerabilidades encontrados mediante la utilización de herramientas de hacking ethical a través del desarrolló scripts.

Objetivo específico:

Comprender el porqué del desarrollo de scripts.
Recopilar información sobre la aplicación y el desarrollo de Scripts
Determinar la mejor utilización de las herramientas hacking ethical.

Referencias:

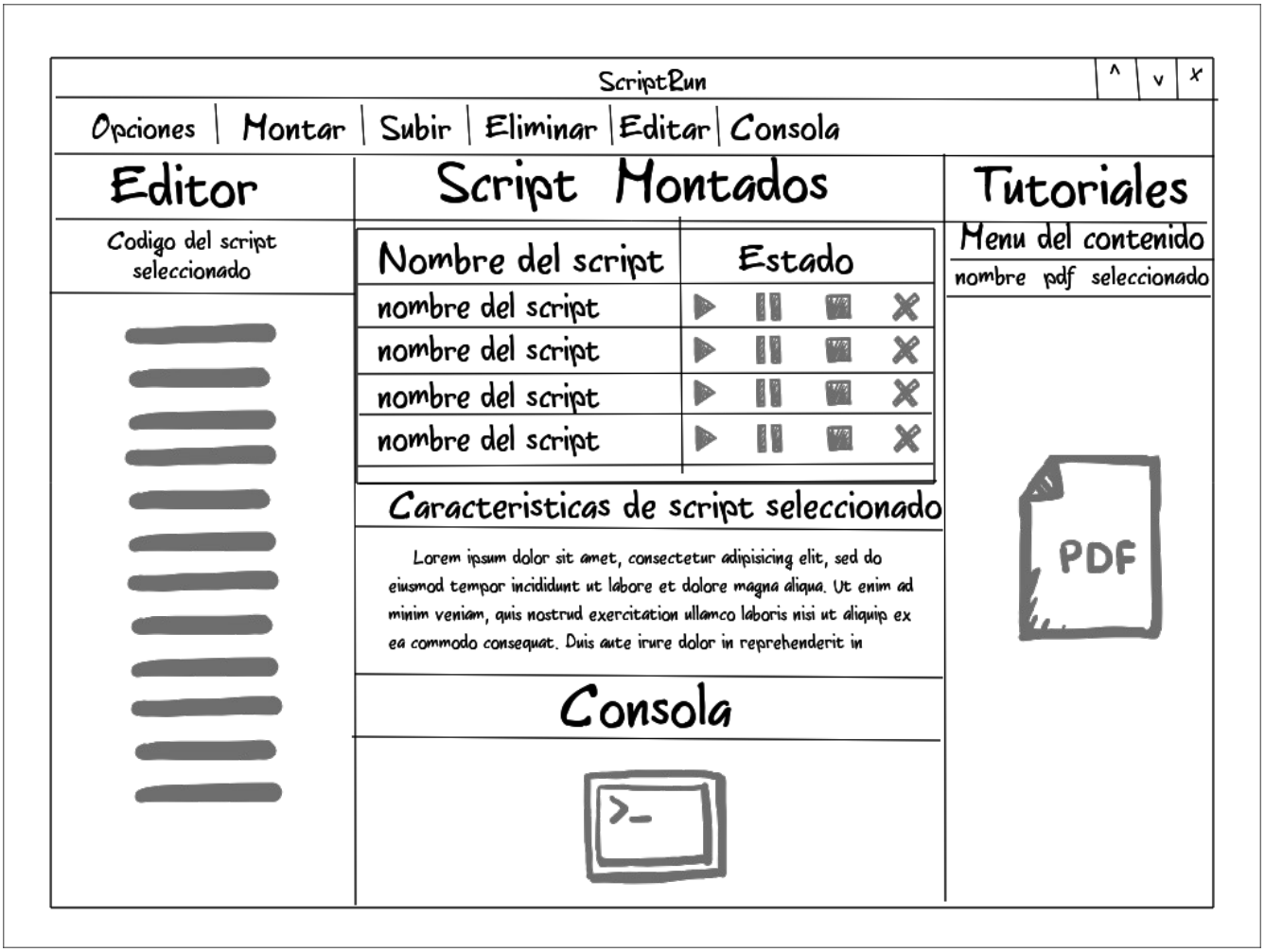
Avgerinos, Thanassis et al. "Automatic Exploit Generation". *Communications of the ACM* 57.2 (2014): 74-84. Web.
Long, Johnny, Bill Gardner, and Justin Brown. "Locating Exploits And Finding Targets". *Google Hacking for Penetration Testers* (2016): 119-123. Web.
Zhang, Meng, Anand Raghunathan, and Niraj K. Jha. "A Defense Framework Against Malware And Vulnerability Exploits". *International Journal of Information Security* 13.5 (2014): 439-452. Web.
Mylonas, Alexis, and Dimitris Gritzalis. "Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software". *Computers & Security* 31.6 (2012): 802-803. Web.
Delgado-Azuara, Francisco, José-Ramón Hilera-González, and Raúl Ruggia-Frick. "Soluciones Para El Intercambio Electrónico De Información De Seguridad Social A Nivel Internacional". *El Profesional de la Informacion* 21.4 (2012): 361-368. Web.
El-Hajj, Wassim et al. "Security-By-Construction In Web Applications Development Via Database Annotations". *Computers & Security* 59 (2016): 151-165. Web. 9 Apr. 2016.

Metodología:

La propuesta dará inicio con el estudio de seguridad básica, encontrando primero los modelos básicos de protección ya que las vulnerabilidades no siempre se dan por fallas de la maquinas sino por fallas humanas en las configuraciones, luego de esto se abarcara el estudio sobre los Scripts, el lenguaje a utilizar y como se desarrollaran, luego se seleccionan las herramientas a utilizar, se hace un estudio sobre estas y sobre las vulnerabilidades que se encuentren. Todo esto se ira implementando en el software scriptRun a través del cual se podrá gestionar los script y el contenido generado en la propuesta.

Actualmente me encuentro en el estudio y aprendizaje de Python ya que este es el software elegido para el desarrollo de scripts, además si se tomara como lenguaje para la propuesta se debe dominar perfectamente, principalmente me encuentro en el desarrollo de una plataforma nombrada ScriptRun

hecha en Python a través de la cual se podrán gestionar los scripts desarrollados, el mock presentado es desarrollado en ninjamock plataforma online para el desarrollo de mocks y sería la pantalla principal:




Lo que tratare a través de ScriptRun es que la persona además de gestionar sus scripts, pueda en la aplicación guardar información acerca de la vulnerabilidad o problema encontrado. Cabe resaltar que la aplicación no estará desarrollada para dispositivos móviles.

Las herramientas de hacking ethical que se implementaran en el estudio serán tratadas sobre lo básico ya que la propuesta está orientada hacia un público principiante, pero se trataran de obtener los mejores resultados, las herramientas propuestas actualmente son las siguientes:

nmap: herramienta para hacer escaneos de red.
nessus: Herramienta para identificar vulnerabilidades.
Metasploit framework: Herramienta usada para explotar vulnerabilidades.
Wireshark y Ettercap: Sniffers utilizados para ver tráfico de redes.
Skipfish: Herramienta que sirve para hacer escáner a sitios web en pre-producción y producción.
Hydra y medusa: Herramienta utilizada para hacer ataques de fuerza bruta.
Nikto y w3af: Herramienta para hacer análisis de sitios web a nivel de servidores.
Mitmproxy: Proxy web diseñado para hacer ataques de hombre en el medio.
Ollydbg: Herramienta para hacer ingeniería inversa.

Everest, Siw y Winaudit: Software para obtener información acerca del hardware.
Digital Forensics Framework, PlainSlight y Bulk Extractor: Herramientas de análisis forense.

Las herramientas planteadas están pensadas para el desarrollo de conocimiento ya que más halla de encontrar vulnerabilidades lo que se quiere es que la persona obtenga información y la pueda utilizar para el desarrollo de los scripts, estos no necesariamente debe responder a una vulnerabilidad si no a las necesidades que la persona pueda tener. Las herramientas planteadas pueden aumentar o cambiar dependiendo de la información que estas arrojan en el estudio para incluirlas en el estado final del proyecto.

El desarrollo de la propuesta es un poco lento debido al gran campo de trabajo que este posee, pero entre más se avance en la propuesta se encontraran nuevas delimitaciones que ayuden al desarrollo de la misma.

Conclusiones:

Las herramientas estan seleccionadas pensando en abarcar la mayoria de temas posibles.

La mayoria de vulnerabilidades no pueden ser solucionadas a traves de Scripts.

El desarrollo de escript no solo se basa en resolver vulnerabilidades, si no que esta enfocado hacia cualquier necesidad que tenga la persona.

Aprendizaje de conceptos básicos de hacking ethical y seguridad, adquisición de metodologías prácticas para encontrar y tratar vulnerabilidades y necesidades con Scripts.

Bibliografía:

Tutoriales de creación de exploits
*by* Corelam Team.

Hacking etico
*by* Carlos Tori.

Redes y Seguridad
*by* Matías Kats.

Ataques contra redes TCP/IP
*by* Joaquín García Alfaro.

Practical Malware Analysis: *the hands-on guide to dissecting malicius software*
*by* Michael Sikorski *and* Andrew honig.