Ingeniería social, hardware y black hackers: armas silenciosas contra la confidencialidad de la información

John Freddy Quintero Tamayo, Martin Camilo Cancelado Ruiz, Martha Fabiola Contreras Higuera
Universidad Nacional Abierta y a Distancia

Fecha de Recepción: 17/02/17 – Fecha de Aceptación:03/04/17

Resumen

La ingeniería social ha venido evolucionando con el paso del tiempo, articulando en cada ocasión sistemas de mayor complejidad a nivel hardware y software con el fin de persuadir y engañar a los usuarios mediante estrategias tecnológicas para entregar información sensible, la cual podrá ser utilizada por el atacante con fines maliciosos y de beneficio personal. En el presente artículo se hace mención de algunas estrategias de tipo hardware de bajo costo, que han estado adoptando mayor aceptación en el ámbito del Phising, en las cuales se demuestra que éste tipo de ataques ha dejado de ser exclusivo bajo el uso de herramientas software, permitiendo llevar a cabo ataques de seguridad más elaborados y que pueden ser realizados por personas que no posean un conocimiento avanzado en este contexto.

Palabras clave: *Phishing, cámara térmica, pineapple nano, Lan Turtle, Ingeniería Social, hacking, confidencialidad de la información, seguridad informática.*

Abstract

Social engineering has evolved over time, articulating on each occasion more complex systems at hardware and software level in order to persuade and deceive users through technological strategies to deliver sensitive information, which can be used by the attacker with malicious purposes and personal benefit. In the present article mention is made of some low-cost hardware-type strategies, which have been adopting greater acceptance in the field of Phishing, in which it is demonstrated that this type of attacks has ceased to be exclusive under the use of software tools, allowing to carry out more elaborate security attacks and that can be carried out by people who do not have advanced knowledge in this context.

Keywords: *Phishing, thermal camera, pineapple nano, Lan Turtle, Social Engineering, hacking, information confidentiality, computer security.*

I. INTRODUCCIÓN

La ingeniería social puede ser considerada como una herramienta que ha sido utilizada por los hackers de manera ética o maliciosa para robar información sensible de las personas [1]. En el desarrollo de tecnologías emergentes relacionadas con la seguridad social algunas empresas como Hak5, keyllama, Flir one entre otras; han realizado grandes esfuerzos en la elaboración de herramientas software que pueden ser de gran ayuda en los procesos de sistemas informáticos. Sin embargo, algunos hackers hacen uso de estas herramientas con fines maliciosos oscureciendo con ello los esfuerzos de éstas empresas en el contexto del Ethical Hacking [2].

Los ataques de ingeniería social se han convertido en una amenaza generalizada para los sistemas informáticos y de comunicaciones, al emplear mecanismos de engaño cada vez más sofisticados, involucrando dispositivos hardware de bajo costo en lugar de los métodos informáticos tradicionales a fin de burlar los controles de seguridad que puedan estar presentes en los sistemas, generando un nuevo mundo de posibilidades para aquellas personas que no poseen conocimientos avanzados de seguridad y que desean formar parte de la comunidad de hackers a nivel mundial [3].

II. METODOLOGÍAS DE ATAQUES BASADOS EN INGENIERÍA SOCIAL HACIENDO USO DE HARDWARE

Cualquier tipo de usuario puede llegar a ser víctima de ataques informáticos haciendo uso de ingeniería social y hardware malicioso sin importar el nivel de experticia en temáticas de seguridad; este tipo de ataques se pueden contrarrestar teniendo conocimiento en la configuración, uso del hardware malicioso y su funcionamiento [4]. Entre las etapas que un hacker puede llegar a realizar para perpetrar algún tipo de ataque, se pueden mencionar [5]:

- ***Entorno:*** En esta fase es importante contemplar el conocimiento y la experticia del atacante allí se debe conocer los sistemas operativos e infraestructura T.I donde se desee generar el ataque.

- ***Recolección de información:*** Fase en la que el atacante identifica los puntos débiles de una organización para poder ejecutar el ataque informático. En este punto el atacante logra recolectar información de la organización para configurar sus equipos posteriormente; en esta fase se puede incluir la técnica

de recolección de información más conocida como footprinting “recolección de información”.

- **Análisis de resultados:** Una vez el atacante logre obtener la información de los puntos débiles de la organización procede a configurar los elementos hardware y software para obtener lo deseado.

- **Generación de ataque:** Por último, el atacante se basará en todo el proceso de entorno, recolección y análisis de información para ejecutar y articular procesos de ingeniería social y de esta forma lograr el mayor porcentaje de éxito en su ataque, también se fusiona los elementos hardware que se definirán más adelante.

Con base en lo descrito anteriormente se procede a mencionar el hardware utilizado por algunos black hackers en el ejercicio de sus labores mal intencionadas. Lo que se pretende buscar como objetivo de este documento es el conocimiento global de los daños que se pueden presentar con hardware de bajo costo y el modus operandi de algunos delincuentes informáticos.

A. Pineapple Nano y Phishing

Figura 1. Red clonada “Ap-rouge” por medio de PineApple nano

Fuente: Los autores.

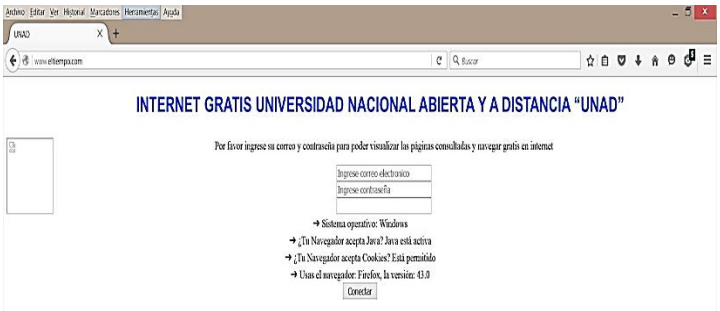
Pineapple es un dispositivo elaborado por la empresa Hak5 que tiene como objetivo auditar las redes inalámbricas de cualquier organización; dentro de su configuración y usabilidad se puede encontrar opciones para configurar un ataque mediante Phishing ya sea para capturar información o generar pánico [6].

La pineapple está elaborada sobre un Arduino pro con dos antenas de 4 dBi cada una; además cuenta con una interfaz gráfica de su sistema operativo donde se configura la ejecución del ataque [7]. Para este ejemplo en particular la Pineapple simula un proxy de conectividad donde proveerá a la víctima de internet mediante un Ap rouge o punto de acceso a internet wifi falso que cuenta con la capacidad de duplicar cualquier SSID “Service Set Identifier” para que la víctima sea confundida e ingrese a la red falsa, la irradiación del Ap rouge se puede visualizar en la Figura 1.

Se observa que existen dos redes con el mismo SSID, para este caso se nombraron como “Alien” el que está señalado en color rojo determina la red falsa y el que está señalado en color azul es la red verdadera teniendo como único punto de comparación el protocolo de autenticación; la falsa tiene acceso director o conocido como red abierta y la verdadera tiene un sistema de autenticación WPA2 “Wifi Protected Access”, estos detalles solo se determinan si el usuario comprende el funcionamiento de estos dispositivos o conoce su alcance [8].

Posterior a la configuración del Ap-rouge toda victima que se conecte a la Pineapple tendrá en pantalla un aviso donde simula un proxy de conectividad allí solicita los datos como correo, contraseña del correo entre otros, el atacante está en la capacidad de configurar y programar el phishing, las pruebas realizadas para este documento se programó una interfaz básica donde una víctima intenta consultar la página www.eltiempo.com y de inmediato emite el phishing simulando el proxy, ver la Figura 2.

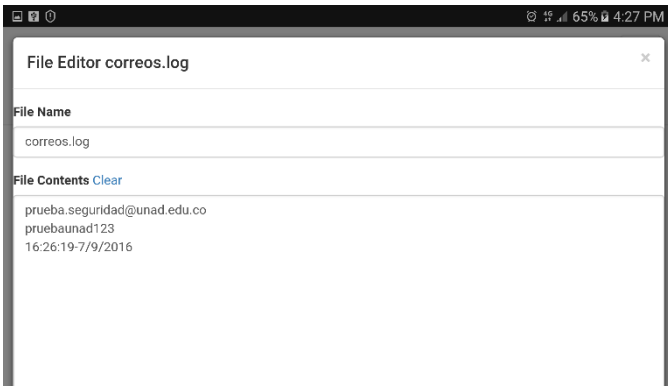
Figura 2. Interfaz phishing del pineapple simulando un proxy de conectividad.



Fuente: Los autores.

Una vez se captura la información solicitada en el falso proxy de conectividad esta se almacenará en la memoria interna del pineapple para posteriormente ser validada por el atacante, la información almacenada se visualiza como se observa en la Figura 3.

Figura 3. Log de contraseñas capturadas con el phishing del Pineapple



Fuente: Los autores.

Este proceso es realmente fácil, y quizás una de las cosas que más peligro genera es la accesibilidad al pineapple porque no requiere de procesos extensos para ser adquirido, de hecho, en convenciones de hackers a nivel mundial como la DEF CON es posible conseguir este tipo de hardware. El pineapple nano cuenta con la capacidad de ser pequeño y fácil de transportar lo que indica que se puede incorporar con el dispositivo móvil y lograr un ataque portable sin ser identificado por personal de seguridad de cualquier organización y/o persona, en la Figura 4 se puede observar la portabilidad y partes de la pineapple nano.

Figura 4. Pineapple Nano Portátil.

Fuente: https://hakshop.com/products/wifi-pineapple?variant=11303796101

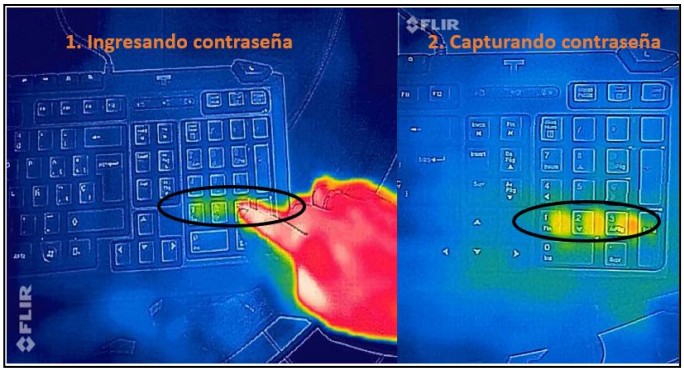
B. Cámara térmica Flir one

La empresa Flir se encarga de elaborar una serie de dispositivos de bajo costo y móviles para identificar los cambios de temperatura por medio de sus cámaras térmicas. Muy lejos de pensar que la teoría de transmisión por calor definida por el matemático Jean Baptiste Joseph Fourier se convertiría en una muy buena metodología para la extracción de contraseñas [3].

La teoría argumenta que aquellas moléculas que tienen mayor energía cinética "temperatura mayor" transfieren su energía directamente a las moléculas adyacentes, las de "temperatura menor" [3] lo que genera una imagen de la transferencia de calor entre los dedos del usuario y el teclado que se encuentra con una temperatura menor mostrando la secuencia de la contraseña.

Los resultados obtenidos en el análisis de un teclado de computadora por medio de la Flir one fueron contundentes en cuanto a mostrar la secuencia de calor emitida por la victima; cabe resaltar que en el transcurso del tiempo el calor se va disipando del teclado por ello se deduce que las teclas de color rojo fueron las últimas en ser digitadas, en cambio las teclas de color más azul fueron las primeras en digitarse esto se puede observar en la Figura 5.

Figura 5. Resultados contraseña captura por medio de Flir One



Fuente: Los autores.

En la Figura 5. Se puede deducir que la contraseña fue 123 digitada de izquierda a derecha. En este tipo de ataques no es muy común encontrar alguna de las metodologías mencionadas anteriormente, dado a que este ataque es de tipo director y está relacionado con la exposición que tenga el usuario con el atacante. Dentro de los análisis de la Flir One se determinó que es más seguro manipular una computadora portátil porque la integración de sus circuitos, tarjeta madre, procesador, memoria RAM entre otros generan continuamente calor lo que hace más difícil el trabajo del atacante por no tener una secuencia de digitación de contraseña como se puede observar en la Figura 6 donde queda demostrado que más del 90% de la computadora y su teclado están expuestos al calor dejando solo una pequeña porción del teclado a temperatura ambiente, esta parte no expuesta por el calor en el teclado se ubica en la parte numérica.

Figura 6. Intento de robo de contraseña mediante el uso de Flir One sobre computadora portátil.

Fuente: Los autores.

Para finalizar cabe mencionar que el atacante deberá tener en cuenta el tipo de dispositivo, porque las últimas versiones no pasarán desapercibidas como la primera versión, por ello hay que tener en cuenta la versión A siendo la más peligrosa como se visualiza en la Figura 7.

Figura 7. Comparación entre la versión antigua de Flir one "A" y la última versión "B".

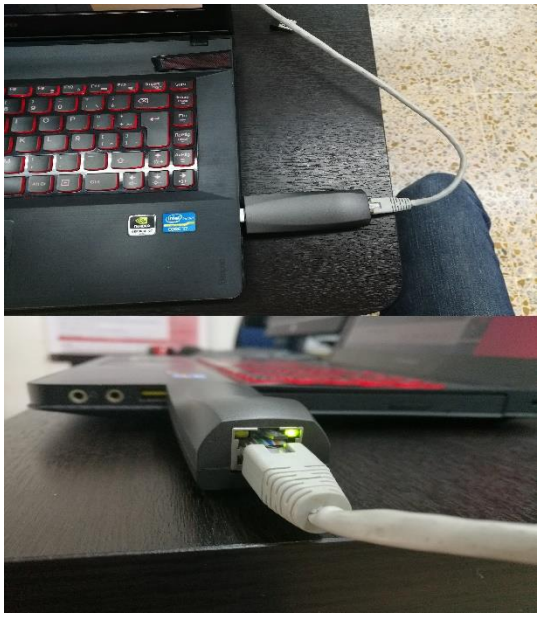
Fuente: http://www.flir.com/Home/

Una de las características de este dispositivo es que puede ser adquirido por sólo 150 dólares poniendo en peligro la confidencialidad de la información de cualquier persona u organización con un bajo costo.

C. Tortuga LAN (LAN Turtle)

Esta herramienta permite acceso a una red de forma remota, siendo una herramienta hardware permite evadir ciertas restricciones de acceso a una red determinada si esta posee medidas de seguridad de acceso externo [6]. El método de uso es de conectar mediante una entrada USB, con acceso a un puerto de cable de tipo RJ45 como se muestra en la figura 8.

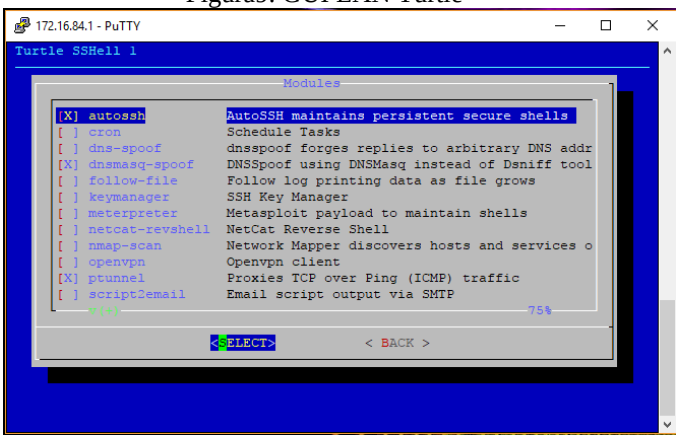
Figura8. LAN Turtle conectada



Fuente: Los Autores

Al estar conectada dentro de la red, esta herramienta en la mayoría de los casos no es detectada por antivirus o firewall, e incluso si su configuración inicia desde el BOOT de cualquier equipo pasa inadvertido independiente de todas las herramientas de software en seguridad, funciona para administración de la red, ethical hacking, ataques de "man in the middle", sniffing, dnsspoof, entre otros [4].

Figura9. GUI LAN Turtle

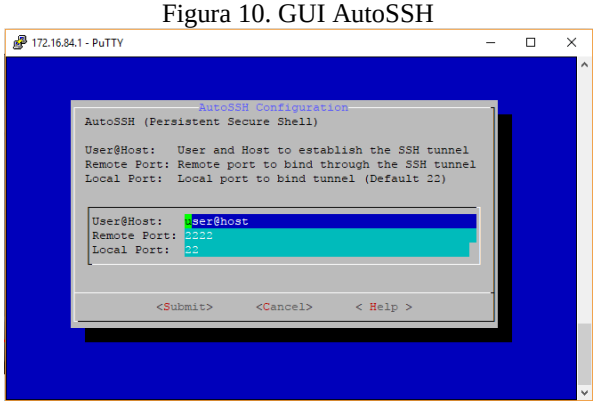


Fuente: Los autores.

Según la Figura 9 podemos observar que la herramienta posee una cantidad de módulos prediseñados, que permiten aplicar las técnicas mencionadas anteriormente. En el caso de realizar sólo captura de tráfico de red se necesita configurar el primer módulo que es el de Autossh, para el

acceso automático cuando arranque el dispositivo a funcionar [9]. Este solicita el acceso del host, preferiblemente una cuenta de servicio de almacenamiento en la nube que permita conexión remota mediante SSH, Figura10.

Figura 10. GUI AutoSSH



Fuente: Los autores.

El sniffing en un medio tradicional, puede ser catalogado como una técnica de escaneo del tráfico de una red sin autorización a ella. Es un método de simple monitoreo de red, que se puede realizar con el propósito de hacer seguimiento a la red observada para posibles accesos sin autorización de terceros, para tener también conocimiento de los ingresos de los usuarios para la óptima gestión de la red [1]. Al ser capturado todo el tráfico de la red y posteriormente analizado, es posible identificar fallas de seguridad existentes, por ejemplo, si se registró un ataque de denegación de servicios, esta herramienta puede haber capturado el tráfico de donde se generó el ataque para realizar el seguimiento de la fuente del ataque [2][10].

La LAN Turtle permite realizar también conexiones VPN cifrando el tráfico de conexión entre el dispositivo y el operador, permitiendo realizar operaciones y tareas de forma remota sin ser detectado [11]. El tamaño del impacto que puede generar se determina por el fin que se requiere para usarla, puede ser para realizar y/o robar información de una entidad u organización, para esto sólo se necesita el medio, en este caso la ingeniería social, para que sea conectada en el lugar donde se desea ser tomada. Esto indica que el nivel de seguridad, no está bien controlada, pues se toma como puente y no es fácil identificar su función o instalación de manera automática, se debe crear las reglas en la red para que identifique este tipo de dispositivos [12].

III. CONCLUSIONES

Los ataques de Phishing y Spoofing utilizan una combinación de técnicas de ingeniería social y técnicas de suplantación para persuadir a los usuarios a entregar información sensible, la cual puede ser utilizada posteriormente con fines maliciosos. Acorde con los resultados obtenidos en el artículo, se pudo evidenciar que existe un gran número de dispositivos hardware de bajo costo, que actualmente permiten realizar diversas estrategias para la generación de ataques a sistemas informáticos mediante el uso de hardware especializado de bajo costo, el cual puede ser adquirido de una manera muy fácil por cualquier persona experta o aficionada en el ámbito de la Seguridad Informática y el Ethical Hacking. En vista de lo anterior, es importante conocer las fortalezas y los alcances que éste tipo de dispositivos puede llegar a ofrecer a fin de proponer en futuros trabajos nuevas estrategias y políticas de seguridad orientadas a resguardar de una mejor forma la información, considerando las nuevas estrategias hardware que han complementado el abanico de alternativas de ingeniería social que pueden llegar a presentarse en un momento específico.

IV. REFERENCIAS

[1] C. E. L. Grande and R. S. Guadron, “Social engineering: The silent attack,” in *2015 IEEE Thirty Fifth Central American and Panama Convention (CONCAPAN XXXV)*, 2015, pp. 1–6.

[2] S. Gupta, A. Singhal, and A. Kapoor, “A literature survey on social engineering attacks: Phishing attack,” in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 2016, pp. 537–540.

[3] A. Cullen and L. Armitage, “The social engineering attack spiral (SEAS),” in *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)*, 2016, pp. 1–6.

[4] R. Heartfield, G. Loukas, and D. Gan, “You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks,” *IEEE Access*, vol. 4, pp. 6910–6928, 2016.

[5] R. Heartfield, G. Loukas, and D. Gan, “An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks,” in *2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA)*, 2017, pp. 371–378.

[6] S. Oriyano, “Retaining Access with Backdoors and Malware,” in *Penetration Testing Essentials*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2017, pp. 143–160.

[7] Z. L. Svehla, I. Sedinic, and L. Pauk, “Going white hat: Security check by hacking employees using social engineering techniques,” in *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2016, pp. 1419–1422.

[8] M. Abu-Tair and S. N. Bhatti, “Introducing IEEE 802.11ac into existing WLAN deployment scenarios,” in *2015 13th International Symposium*

on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), 2015, pp. 30–35.

[9] C. Atwell, T. Blasi, and T. Hayajneh, "Reverse TCP and Social Engineering Attacks in the Era of Big Data," in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 2016, pp. 90–95.

[10] E. Vattapparamban, B. S. Ciftler, I. Guvenc, K. Akkaya, and A. Kadri, "Indoor occupancy tracking in smart buildings using passive sniffing of probe requests," in *2016 IEEE International Conference on Communications Workshops (ICC)*, 2016, pp. 38–44.

[11] E. Vattapparamban, I. Guvenc, A. I. Yurekli, K. Akkaya, and S. Uluagac, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2016, pp. 216–221.

[12] A. A. Rao, K. Sujatha, A. Uday, and N. N. Mani, "Idle lock based privacy preserving secured web browser," in *2015 International Conference on Man and Machine Interfacing (MAMI)*, 2015, pp. 1–4.

V. BIOGRAFÍA

M.Sc. John F. Quintero Tamayo, Ingeniero de Sistemas, especialista en Seguridad Informática, egresado de la universitat Oberta de Catalunya como Magister en Seguridad Informática obteniendo matrícula de honor en su proyecto de grado de finalización de Master.

Su experiencia profesional está enfocada a la investigación en el campo de seguridad informática, actualmente trabaja en la universidad Nacional Abierta y a Distancia "UNAD" como docente de la Especialización en Seguridad Informática y líder en investigación en el mismo campo; las temáticas de experticia se enfocan a: Análisis de seguridad, hacking ético, pentesting, ingeniería social.

Esp. Martín Camilo Cancelado Ruiz, Ingeniero de sistemas de la Universidad Cooperativa de Colombia, seccional Bucaramanga. Especialista en seguridad Informática de la Universidad Pontificia Bolivariana seccional Bucaramanga. Auditor interno ISO 27001:2013. Docente e investigador de la Universidad Nacional Abierta y a Distancia, asesor de proyectos de grado del postgrado en la Especialización en Seguridad Informática de la misma universidad

M.Sc.(c). Martha Fabiola Contreras H. Ingeniera Electrónica (Universidad de Pamplona), Especialista en Telecomunicaciones (Universidad Industrial de Santander) y Magister en Ingeniería área Telecomunicaciones (En curso con la Universidad Pontificia Bolivariana). Docente e Investigadora desde el año 2010 en la UNAD.