DOCUMENTO CONFIDENCIAL

binario

IT Advisory Services

INFORME TÉCNICO:

Segundo Escaneo y Test de Penetración – Red Electoral

- **Escaneo de 02 Máquinas de Voto Electrónico**

SERVICIO DE ETHICAL HACKING EG 2016

Adjudicación Simplificada Nº 029-2016-EG-ONPE

Abril 2016

QUALITY CONTROL binario PASSED

Contenido

1. Introducción

El presente documento es parte del resultado correspondiente al Segundo Escaneo y Test de Penetración a la Red Electoral - Servicio Ethical Hacking EG 2016 - Adjudicación Simplificada N° 029-2016-EG-ONPE, el cual incluyó el escaneo de dos (02) Equipos de Voto Electrónico proporcionados por la ONPE.

La evaluación fue realizada el día 06.ABR.2016, en las oficinas de la ONPE Jr. Washington 1894 Of. 707, Cercado de Lima, con la participación del personal de la Gerencia de Tecnología e Informática Electoral de la ONPE.

El Servicio de Ethical Hacking EG 2016 abarca el escaneo remoto en caja gris (con limitada información acerca del objetivo de ataque, sin contacto físico pleno) de la Red Electoral, Red Administrativa y Aplicaciones Web. Dentro de este contexto y como caso especializado se realizó el escaneo de 02 Máquinas de Voto Electrónico, dado que dichos equipos no cuentan conexión física de red (mediante cables), se procedió a intentar establecer conexión mediante la red inalámbrica con la finalidad de conectarse y efectuar el escaneo.

El escaneo fue realizado a las siguientes 02 máquinas de voto electrónico proporcionadas por la ONPE el día 06.ABR.2016:

a. Estación de Comprobación de Identidad

Inventario ONPE: INV 2015 0026790

Código patrimonial: Tableta Pad 740894931782

Número de serie del fabricante: R52GC0KDJET

b. Cabina de Votación Electrónica

Inventario ONPE: INV 2015 006142

Código patrimonial: Tableta Pad 740894934053

Número de serie del fabricante: R52GC0L8FGZ

Como parte del desarrollo del trabajo, no se efectuó:

- Evaluación en caja blanca con privilegios de administrador de los controles de seguridad implementados a nivel de sistema operativo o servicios como: permisos de archivos y directorios, perfiles y grupos de usuarios, bitácoras (log) de auditoría, configuración segura de seguridad de sistema operativo y servicios recomendada según estándares de seguridad (NIST, CIS, fabricantes de cada producto).
- Revisión de código fuente de aplicaciones.
- Descompilación o análisis binario de: micro código de firmware y librerías de sistema operativo.
- Pruebas de intrusión física mediante dispositivos extraíbles: USB, Firewire, Smart Cards.
- Evaluación de Ingeniería Social.

2. Reporte de Escaneo de 02 Equipos de Voto Electrónico

2.1. Ámbito de aplicación

De acuerdo a lo especificado en los Términos de Referencia del servicio, en donde se solicita en el alcance[1] el escaneo de la Red Electoral, Red Administrativa y análisis Aplicaciones Web, bajo modalidad Caja Gris; asimismo el escaneo de equipos de Voto Electrónico, se procedió a efectuar el escaneo de 02 equipos puestos a disposición para dichas pruebas de seguridad.

La aplicación del escaneo comprende la evaluación a nivel de red, quedando fuera del alcance el acceso físico o manipulación física de los equipos de Voto Electrónico, por corresponder a un análisis en Caja Blanca o Auditoría.

2.2. Escenario de Pruebas

Para que se efectúe un escaneo de los equipo de voto electrónico se requiere establecer remota con el equipo, teniendo como alternativas la conexión inalámbrica (Wi-Fi) y Blutooth.

2.3. Metodología

a. Escaneo del espectro inalámbrico Wi-Fi con la finalidad de detectar la interfaz de red inalámbrica del equipo, en modo cliente o access point, y posteriormente establecer conexión.

b. Escaneo del espectro inalámbrico Bluetooh con la finalidad de detectar la interfaz blutooth del equipo y posteriormente establecer conexión.

c. En caso de establecer conexión con el equipo de Voto Electrónico, se procederá a ejecutar la metodología de Ethical Hacking de Infraestructura descrita en el presente documento, de acuerdo a su aplicabilidad por cada fase.

2.4. Equipos puestos a disposición para la evaluación

La ONPE puso a disposición de los siguientes 02 equipos de Voto Electrónico:

1. Estación de Comprobación de Identidad

Inventario ONPE: INV 2015 0026790

Código patrimonial: Tableta Pad 740894931782

Número de serie del fabricante: R52GC0KDJET

2. Cabina de Votación Electrónica

Inventario ONPE: INV 2015 006142

Código patrimonial: Tableta Pad 740894934053

Número de serie del fabricante: R52GC0L8FGZ

2.5. Escaneo del espectro inalámbrico Wi-Fi y Blutooth

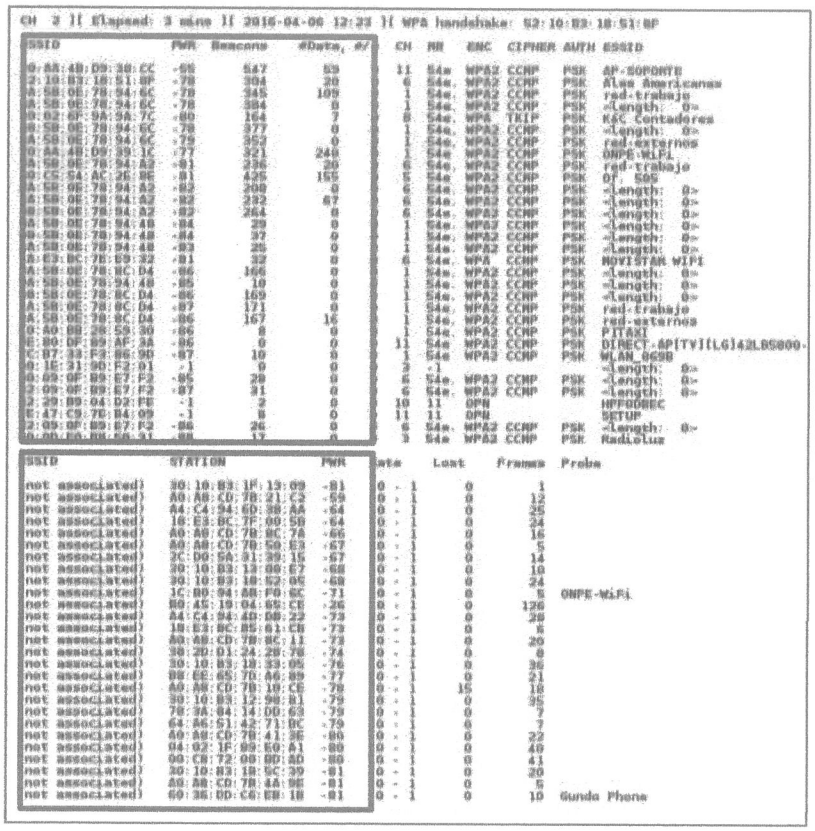
a. Configuró el escaneo del espectro inalámbrico Wi-Fi y Blutooh desde un equipo portátil y dispositivo móvil a una distancia aproximada de 25 cm de la Estación de Comprobación de Identidad y a 80 cm de la cabina de votación electrónica, como se muestra en la siguiente fotografía:

[1] VI.1 Alcance de los Términos de Referencia. Adjudicación Simplificada 029-2016-EG-ONPE Primera Convocatoria.

Escaneo de red inalámbrica (Wi-Fi, Bluetooh)

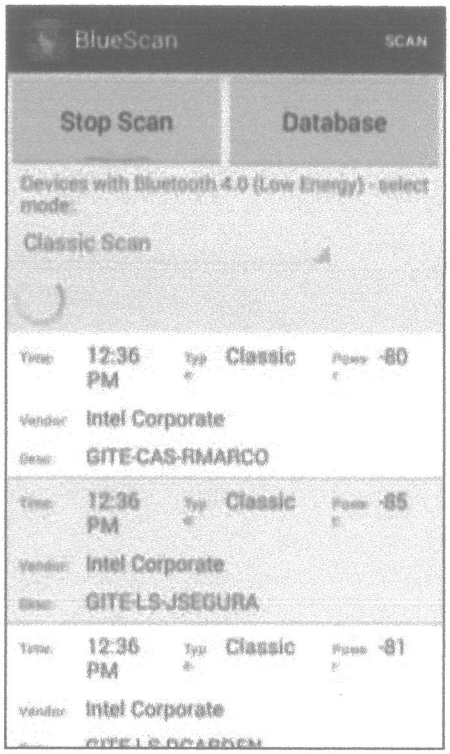
b. Se solicitó al personal de la ONPE que efectúen los procesos de Inicialización y Votación.

c. Mediante la herramienta Aircrack-ng, específicamente Airodump-ng se efectuó la exploración completa en todos los canales en búsqueda de la señal inalámbrica Wi-Fi de los equipos en evaluación, no encontrándose la señal de la interfaz inalámbrica, ya sea como cliente o como access point:



Se adjunta al presente informe los archivos con las capturas en formato PCAP de las exploraciones realizadas.

d. Mediante la herramienta de escaneo Blutooth BluScan se efectuó la exploración en búsqueda de la señal inalámbrica Blutooth de los equipos en evaluación, no encontrándose dicha señal.



2.6. Resultados

Para los dos (02) equipos evaluados, no se obtuvo una vía de acceso Wi-Fi o Blutooth, por consiguiente no fue posible establecer una conexión de red remota para efectuar un escaneo.