Wifi MÓDULO: PROCESO DE EVALUACIÓN DE RIESGOS

Taller 1

Actividad de aprendizaje:

El siguiente taller tiene como objetivo que el Aprendiz identifique y estime los factores de probabilidad e impacto ante el riesgo presentado en situaciones ejemplos.

Para esta actividad el aprendiz deberá:

- Utilizar la calculadora CVSS https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- Utilizar la calculadora owasp risk rating https://www.owasp-risk-rating.com/

Nota: material de apoyo para guiar a los alumnos https://owasp.org/www-community/OWASP_Risk_Rating_Methodology , https://www.youtube.com/watch?v=FL-11NNquQA , https://www.first.org/cvss/user-guide

Actividades del taller

La empresa bpantich es una empresa que surgió hace cinco años y recientemente obtuvo un mega contrato a nivel nacional, por lo tanto, recibió una gran inyección de dinero como anticipo y dentro de los requisitos de ese contrato tiene la centralización de la información en la oficina principal de Bogotá y la atención de público aproximado a 500 personas diarias. El público debe contar con acceso a internet para las labores que haga (asesores externos, otros) o como entretenimiento mientras espera a que sea atendido. La empresa para cubrir estos requisitos implementó un esquema de red sencillo sin una debida Consultoría y mecanismos de seguridad, por eso está expuesta ante posibles ciberataques de forma local o remota.

Situación 1:

La empresa configuro una red inalámbrica pública para todos los asistentes a la oficina de Bogotá sean asesores o clientes, la red inalámbrica no tiene contraseña y está conectada al switch principal de comunicación:

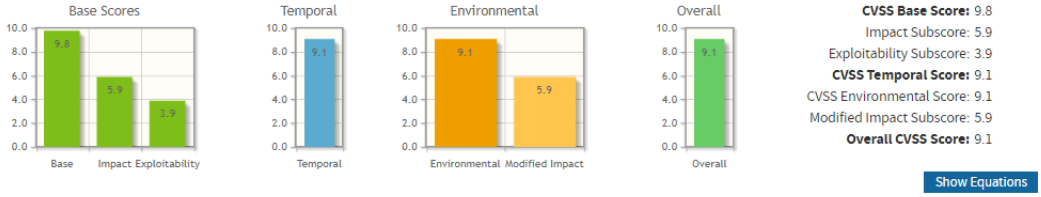
1. Calcule la probabilidad e impacto de un ataque sobre esa red, puede tomar los siguientes ejemplos

- Captura de tráfico
- Ataques de autenticación
- Escaneos de puertos
- Denegación de servicio

R:/ el estudiante debería utilizar las calculadoras y estimar el riesgo, probabilidad e impacto, acá no se evalúa los puntajes sino el uso de las herramientas y la capacidad para estimar o calcular las situaciones, se anexa ejemplo de un cálculo o estimación.

Joaquim Chagas Neto 07/02/2024

such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 9.8
Impact Subscore: 5.9
Exploitability Subscore: 3.9
CVSS Temporal Score: 9.1
CVSS Environmental Score: 9.1
Modified Impact Subscore: 5.9
Overall CVSS Score: 9.1

Show Equations

CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | High (AC:H)

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | Required (UI:R)

Scope (S)*
Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*
None (A:N) | Low (A:L) | High (A:H)

* - All base metrics are required to generate a base score.

Comentarios:

Al estar conectada al switch principal la confidencialidad, integridad y disponibilidad es elevada. Siendo el vector de ataque una red pública sin contraseña la complejidad de atacarla es baja o nula, no se requiere privilegios y tampoco interacción del usuario para explotar una vulnerabilidad.

Situación 2:

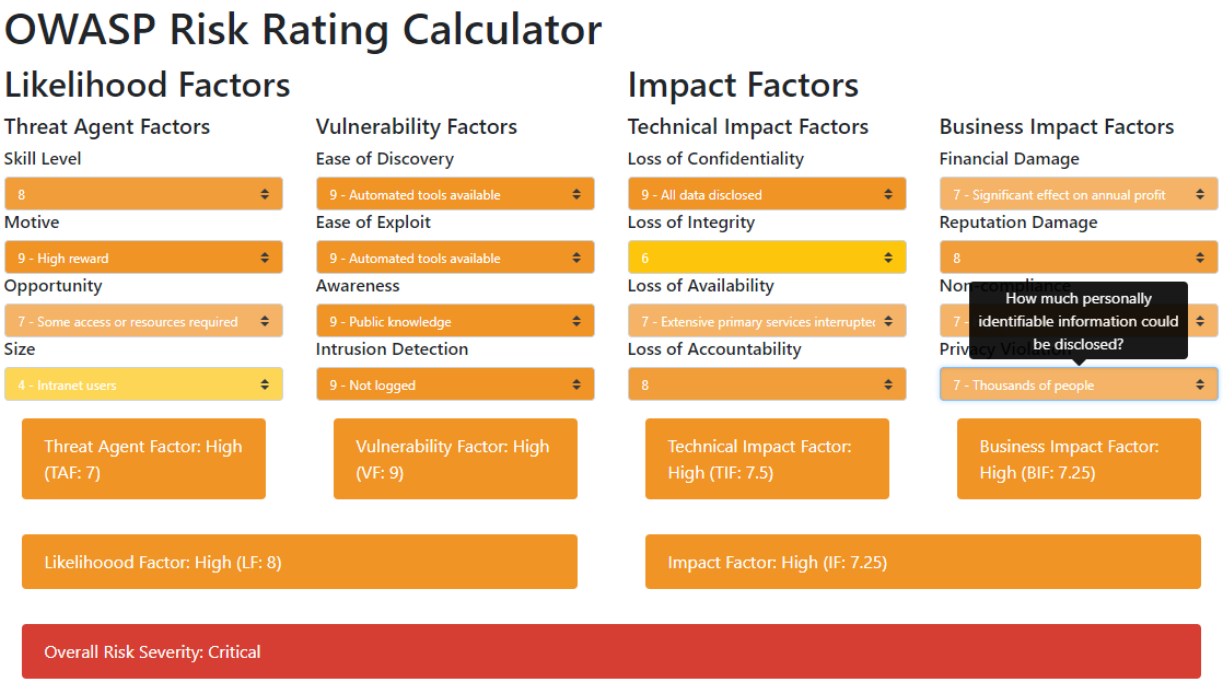
La empresa configuro una red inalámbrica pública para los clientes y una privada para el público asesor de Bogotá, la red inalámbrica pública está segmentada y no ve la red interna pero la red privada está mal segmentada y está conectada al switch principal de comunicación:

2. Calcule la probabilidad e impacto de un ataque sobre la red privada, puede tomar los siguientes ejemplos

- Captura de tráfico
- Ataques de autenticación
- Escaneos de puertos
- Denegación de servicio
- Robo de información
- Escaneos de vulnerabilidades
- Explotación de vulnerabilidades

Joaquim Chagas Neto 07/02/2024

R:/ el estudiante debería utilizar las calculadoras y estimar el riesgo, probabilidad e impacto, acá no se evalúa los puntajes sino el uso de las herramientas y la capacidad para estimar o calcular las situaciones, se anexa ejemplo de un cálculo o estimación.



En este caso al estar mal segmentada la red interna. Se podría atacar, pero involucra una mayor habilidad para poder ejecutar el ataque. Se podrá descubrir el riesgo asociado a la red mediante herramientas automatizadas, también se podrá explotar la vulnerabilidad con otras herramientas. El awareness se relaciona a la capacidad de poder reconocer la vulnerabilidad en este caso público. No se necesita estar logueado en la red produciendo un riesgo alto de vulnerabilidad.

Si se logra explotar la vulnerabilidad la triada CIA se ve comprometida, sobre todo la confidencialidad y la disponibilidad de la información. Teniendo consecuencias a nivel de negocio en materia financiera, reputacional e información relacionada con las personas de esa empresa.

Esto podría concluir en un riesgo crítico para la empresa.

Joaquim Chagas Neto 07/02/2024