

TABLA DE CONTENIDOS

	página
Dedicatoria	I
Tabla de Contenidos	II
Índice de Figuras	VII
Índice de Tablas	IX
Resumen	x
1. Introducción	11
1.1. Contexto del Proyecto	11
1.2. Definición del Problema	12
1.3. Objetivos	14
1.3.1. Objetivo General	14
1.3.2. Objetivos Específicos	15
2. Antecedentes	16
2.1. Conceptos Generales	16
2.1.1. Seguridad Informática	16
2.1.2. Confidencialidad	16
2.1.3. Disponibilidad	17
2.1.4. Integridad	17
2.1.5. Activos	17
2.1.6. Amenazas	18
2.1.7. Vulnerabilidades	18
2.1.8. Exposición	18
2.1.9. Riesgo	18
2.1.10. Controles	19
2.1.11. Exploit	19
2.1.12. Protocolo ARP	19
2.1.13. XSS	19

2.1.14. SQLi	20
2.2. Etapas de un Análisis de Seguridad	20
2.2.1. Alcance y Términos del Análisis	20
2.2.2. Recolección de Información	20
2.2.3. Análisis de Vulnerabilidades	21
2.2.4. Explotación de Vulnerabilidades	22
2.2.5. Post Explotación del Sistema	22
2.2.6. Generación de Informe	22
2.3. Vulnerability Assessment	23
2.4. Penetration Testing (Pentesting)	24
2.5. Cifrado	25
2.5.1. Cifrado Simétrico	25
2.5.2. Cifrado Asimétrico	25
2.5.3. Certificados Digitales	26
2.6. Ambiente de Desarrollo	26
2.6.1. Sistema Operativo	26
2.6.2. Hardware	27
2.6.3. Lenguaje de Desarrollo	27
2.6.4. Netcat	27
2.6.5. Route	28
2.7. Herramientas	28
2.7.1. ARP-Scan	28
2.7.2. GNU Wget	29
2.7.3. GnuPG	29
2.7.4. Ifconfig	30
2.7.5. Nessus	30
2.7.6. Netdiscover	31
2.7.7. Nmap	31
2.7.8. OpenVAS	31
2.7.9. SendMail	32
2.8. OpenVAS vs Nessus	32
3. Metodología	34
3.1. Preparación e Investigación	34

3.1.1.	Metodologías y Conocimientos	34
3.1.2.	Herramientas	34
3.1.3.	Script	35
3.1.4.	Securización y Envío	35
3.1.5.	Desarrollo	36
3.1.6.	Evaluación	36
4.	Desarrollo	38
4.1.	Diseño	38
4.1.1.	Etapas de Evaluación	38
4.1.2.	Securización de Información	40
4.1.3.	Envío de Información	41
4.1.4.	Flujo de trabajo	41
4.2.	Implementación	44
4.2.1.	Host	45
4.2.2.	Variables Globales	47
4.2.3.	Funciones de Apoyo	47
4.2.4.	Funciones Primarias	49
4.2.5.	Flujo de Ejecución	56
5.	Evaluación	57
5.1.	Escenario 1	58
5.1.1.	Configuración de Hosts	58
5.1.2.	Pruebas Etapa Identificación de Puertos y Servicios	61
5.1.3.	Pruebas Etapa Identificación de S.O.	62
5.1.4.	Pruebas Etapa Identificación de Vulnerabilidades	63
5.2.	Escenario 2	63
5.2.1.	Configuración de Hosts	64
5.2.2.	Pruebas Etapa Identificación de Puertos y Servicios	67
5.2.3.	Pruebas Etapa Identificación de S.O.	67
5.2.4.	Pruebas Etapa Identificación de Vulnerabilidades	68
5.3.	Escenario 3	69
5.3.1.	Configuración de Hosts	70
5.3.2.	Pruebas Etapa Identificación de Puertos y Servicios	72

5.3.3. Pruebas Etapa Identificación de S.O.	73
5.3.4. Pruebas Etapa Identificación de Vulnerabilidades	74
5.4. Análisis	75
6. Conclusiones y Trabajo Futuro	80
6.1. Conclusiones	80
6.2. Trabajo a Futuro	81
Bibliografía	83
Anexos	
A: Escenario 1	88
A.1. Puertos y Servicios	88
A.1.1. Laptop0	88
A.1.2. PC0	89
A.1.3. PC1	89
A.1.4. PC2	90
A.1.5. PC3	90
A.1.6. PC4	91
B: Escenario 2	92
B.1. Puertos y Servicios	92
B.1.1. Laptop0	92
B.1.2. Laptop1	93
B.1.3. PC0	94
B.1.4. PC1	94
B.1.5. PC2	95
B.1.6. PC3	95
B.1.7. PC4	96
B.1.8. PC5	97
C: Escenario 3	98
C.1. Puertos y Servicios	98
C.1.1. Laptop0	98
C.1.2. Laptop1	99

C.1.3. PC0	100
C.1.4. PC1	100
C.1.5. PC2	101
C.1.6. PC3	101
C.1.7. PC4	102
C.1.8. PC5	103

ÍNDICE DE FIGURAS

	página
1.1. Proceso de Evaluación Automatizado.	13
2.1. CVEs descubiertas por OpenVAS y Nessus.	33
4.1. Flujo de trabajo de IVScript.	41
4.2. Atributos y métodos del objeto Host.	45
5.1. Primer escenario de evaluación.	59
5.2. Segundo escenario de evaluación.	64
5.3. Tercer escenario de evaluación.	69
5.4. Tiempo de ejecución de la etapa de Identificación de Puertos y Servicios en cada escenario.	76
5.5. Tiempo de ejecución de la etapa de Identificación de S.O. en cada escenario.	77
5.6. Tiempo de ejecución de la etapa de Identificación de Vulnerabilidades en cada escenario.	78
A.1. Puertos de Laptop0.	88
A.2. Puertos de PC0.	89
A.3. Puertos de PC1.	89
A.4. Puertos de PC2.	90
A.5. Puertos de PC3.	90
A.6. Puertos de PC4.	91
B.1. Puertos de Laptop0.	92
B.2. Puertos de Laptop1.	93
B.3. Puertos de PC0.	94
B.4. Puertos de PC1.	94
B.5. Puertos de PC2.	95
B.6. Puertos de PC3.	95
B.7. Puertos de PC4.	96
B.8. Puertos de PC5.	97

C.1. Puertos de Laptop0.	98
C.2. Puertos de Laptop1.	99
C.3. Puertos de PC0.	100
C.4. Puertos de PC1.	100
C.5. Puertos de PC2.	101
C.6. Puertos de PC3.	102
C.7. Puertos de PC4.	102
C.8. Puertos de PC5.	103

ÍNDICE DE TABLAS

	página
5.1. Equivalencia de equipos utilizados y evaluados en los tres escenarios.	57
5.2. Equivalencia de equipos utilizados y no evaluados en los tres escenarios.	58
5.3. Cantidad de puertos descubiertos por herramienta, para cada host en el Escenario 1.	62
5.4. Sistemas operativos detectados para cada host vs sistema operativo conocido, en el Escenario 1.	62
5.5. Vulnerabilidades que afectan a los hosts en el Escenario 1, clasificadas por nivel.	63
5.6. Cantidad de puertos descubiertos por herramienta, para cada host en el Escenario 2.	67
5.7. Sistemas operativos detectados para cada host vs sistema operativo conocido, en el Escenario 2.	68
5.8. Vulnerabilidades que afectan a los hosts en el Escenario 2, clasificadas por nivel.	68
5.9. Cantidad de puertos descubiertos por herramienta, para cada host en el Escenario 3 subred 192.168.0.0/24.	72
5.10. Cantidad de puertos descubiertos por herramienta, para cada host en el Escenario 3 subred 192.168.1.0/24.	73
5.11. Sistemas operativos detectados para cada host vs sistema operativo conocido, en el Escenario 3 subred 192.168.0.0/24	73
5.12. Sistemas operativos detectados para cada host vs sistema operativo conocido, en el Escenario 3 subred 192.168.1.0/24	74
5.13. Vulnerabilidades que afectan a los hosts en el Escenario 3 subred 192.168.0.0/24, clasificadas por nivel.	74
5.14. Vulnerabilidades que afectan a los hosts en el Escenario 3 subred 192.168.1.0/24, clasificadas por nivel.	75