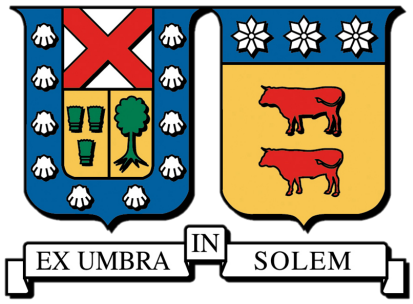
Keywords: 1

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

DEPARTAMENTO DE INFORMATICA

CIUDAD - CHILE



METODOLOGIAS DE ANALISIS EN SEGURIDAD PARA APLICACIONES WEB

DANIEL FRANCISCO TAPIA RYBERTT

MEMORIA DE TITULACIÓN PARA OPTAR AL TÍTULO DE INGENIERO CIVIL EN INFORMATICA.

PPROFESOR GUÍA : RAUL MONGE

ABRIL 2017

TABLE OF CONTENTS

List of Tables

Table **Page**

List of Figures

Figure **Page**

CHAPTER 1

INTRODUCCION

Para esta primera parte se presentara la problematica en el tema de seguridad en ambientes web, las soluciones que se han aplicado y las herramientas que se usan para detectar vulnerabilidades de seguridad.

1.1 Entorno Actual

Actualmente 1/3 del GDP Mundial esta concentrado en la web, sitios de comercio como Amazon.com, Ebay.com y Alibaba.com entre otros dominan el mercado comercial como nunca antes, los bancos han agilizado sus servicios atraves de apliaciones web y desde pequenos hasta grandes negocios son beneficiados por el uso de sistemas de informacion para aumentar su productividad.

Con el aumento de la integracion de la web en nuestra vida cotidiana, en igual proporcion a subido los ataques a estos sistemas. El resguardo de la informacion, privacidad como tambien protejerse de atacantes es una de los problemas mas grandes en servicios web en la actualidad. Asegurar que las aplicaciones web sean lo mas seguras posibles sea a convertido en una necesidad y esta dejando de ser un caracteristica atractiva de una aplicacion.

Una de las formas de resguardar las aplicaciones es atraves de un proceso de pruebas, denominado penetration testing o Pentest. Este proceso de pruebas implica correr softwares de reconocimiento para obtener informacion de el objetivo, usar esta informacion para detectar fallas dentro de la aplicacion o por la periferia, para luego encontrar alguna vulnerabilidad que permita ingresar al sistema.

Existen varias metodologias para un buen pentest. [1]

1. OWASP testing guide
2. PCI Penetration testing guide

3. Penetration Testing Execution Standard
4. NIST 800-115
5. Penetration Testing Framework
6. Information Systems Security Assessment Framework (ISSAF)
7. Open Source Security Testing Methodology Manual (“OSSTMM”)

1.2 Metodologias

Para poder conducir un pentest optimo, se debe recordar las cinco fases de analisis y recopilamiento de informacion. Resumidas a continuacion.

1. Footprinting
2. Scanning
3. Exploit
4. Payload
5. Persitence

1.2.1 Footprinting

La fase de footprinting consiste en buscar informacion publica de el objetivo a analisar, cuentas de linkedin, facebook, twitter, registros publics gubernamentales etc. Toda la informacion recopilada en esta fase puede ser muy valiosa en el futuro.

1.2.2 Scanning

La fase de escanear consiste en correr port scanners como Nmap para intentar enumarar las infraestrutura del objetivo, puertos publicos o privados, e intentar ver que servicios se albergan detras de estos junto con la version de ese software. Esta informacion es muy importante al momento de querer correr algun exploit sobre el objetivo.

1.2.3 Exploit

La fase de exploit consiste en analizar los datos recopilados en las dos fases anteriores e intentar encontrar una falla o vulnerabilidad que permita la ejecucion de codigo o extraccion de informacion no autorizada. Tambien es posible que al tener las versiones y servicios de los endpoints, encontrar una vulnerabrZilidad ya reportarda y que el objetivo no a actualizado.

1.2.4 Payload

La fase de payload consiste en que una vez encontrada la falla de seguridad o vulnerabilidad, usarla para conseguir acceso al sistema, y subir un script o un programa que ejecute el ataque deseado, dentros de estos ataques existen scripts malisios, malware, shells reversos etc.

1.2.5 Persistence

La fase de persistencia consiste en que una vez que se haya ejecutado el payload se debe instaurar una forma de acceso a la maquina sin pasar por la vulnerabilidad encontrada, mas bien levantar servicios o conectarse a servidores externos controlados por el atacante que permitan el facil acceso a la maquina atacada en caso de que la vulnerabilidad sea arreglada.

1.3 Herramientas

Para poder ejecutar un pentest eficiente es necesario el uso de herramientas que agilizen el proceso de obtencion de datos y colaboren en encontrar vulnerabilidades dentro de cualquier ambiente y aplicacion. A continuacion se presentara una coleccion de herramientas estandar en la industria de seguridad en informatica.

1.3.1 Scanners

1.3.1.1 Vulnerabilidad

1. Nessus [Multi]
   Nesus es un no de los scanners de vulnerabilidades mas usados por auditores y analistas de seguridad en el mundo, los usuarios pueden correr multiples scans, crear politicas de seguridad, generar scans por horario y generacion de reportes via email. Tambien integra con una gran mayoria de productos de seguridad y hardware usado por profesionales.

   Permite el analisis en ambientes virtualizados y plataformas en la nube, como tambien deteccion de malware y el uso de botnets.

2. OpenVAS [Win, Unix]

   El Open Vulnerability Assessment System (OpenVAS) es un framework compuesto de varios servicios y herramientas que ofrecen una comprensiva y poderosa plataforma de escanear y manejo de vulnerabilidades.

   El escaner esta acompanado por un constante flujo de mejoras de la NVT (Network Vulnerability Tests) con un total de 47.000 para Junio, 2016.

3. Core Impact [Win] Core impact no es barato, pero es considerado ampliamente como la herramienta de explotación mas potente en la actualidad. Contiene una gran base de datos

de exploits profesionales, tambien tiene mecanismos como hacer pivotes entre maquinas infectadas atraves de tuneles encriptados.

4. Nexpose [Win,Unix]

1.3.1.2 Web

1. Burp Suite [Multi] Burp Suite es un servidor proxy que permite la captura y forward de paquetes para poder hacer crawling sobre una pagina para poder mapearla
2. Nikto [Multi]
3. w3af [Multi]
4. WebScarab [Multi]
5. sqlmap [Multi] Permite correr conocidos strings de sql que permiten analizar si existen vulnerabilidades del tipo sql injection, su fuerte es blind sql injection pero permite tambien in-band sql injection y out-of-band.
6. skipfish [Multi]
7. Acunetix WVS [Multi]
8. AppScan [Multi]

1.3.2 Sniffers

1. Wireshark [Multi] Analizador de datos en la capa de red, permite la captura de paquetes y analisis de headers y metadata en un flujo de datos.
2. Cain and Abel [Win]
3. Tcpdump [Multi]
4. Ettercap [Multi] Herramienta que permite montar ataques MitM (Man in the Middle) quedo descontinuada una vez que SSL se hizo mas popular e implementado a nivel global. Ultimamente ataques que permiten descarcatar el certificado SSL, a convertido a esta herramienta util nuevamente.
5. NetStumbler [Win]
6. dsniff [Multi]
7. NetworkMiner [Win]

1.3.3 Exploitation

1. Metasploit [Multi] Framework de exploits y payloads que permite el facil manejo de estas. Conocido como uno de los mejores frameworks del mundo para penetration testing. Permite generacion de scripts y persistencia atraves de pivots y herramientas propias del framework como Rail Gun.
2. w3af [Multi]
3. Core Impact [Win]
4. Social Engineer Toolkit [Multi]
5. BeEF [Multi]

1.3.4 Crackers

1. Aircrack-ngp [Unix] El suite de Aircrack permite el analisis de redes Wifi en la banda 2.4 para atacar el estandar 802.11, esta herramienta permite escanear el aire por redes en el vecindario, captura e injeccion de paquetes, levantar access points falsos y crackear passwords de la red.
2. Cain and Abel [Win]
3. John the Ripper [Multi] John es la herramienta open source mas popular para crackear passwords a traves de fuerza bruta, permite generacion de diccionarios para atacar como tambien reemplazos por patron para aumentar aun mas el espectro de cobertura por los diccionarios.
4. THC Hydra [Unix] Hydra es otro password cracker que recibe su nombre por su capacidad de generar threads para acelerar el proceso de fuerza bruta hacia servicios (1 cabeza de la hydra = un hilo de procesamiento). Permite ataques hacia servidores ssh, ftp, http, smtp entre otros.
5. ophcrack [Multi]
6. Medusa [Unix]

1.4 System Specifications

All programs and builds will be done under my own personal computer which is an ASUS ZenBook UX305, Processor Intel Core ™

CHAPTER 2

APKTOOL

A tool for reverse engineering 3rd party, closed, binary Android apps. It can decode resources to nearly original form and rebuild them after making some modifications. It also makes working with an app easier because of the project like file structure and automation of some repetitive tasks like building apk, etc.

It is NOT intended for piracy and other non-legal uses. It could be used for localizing, adding some features or support for custom platforms, analyzing applications and much more.

2.1 Application

2.1.1 Features

1. Disassembling resources to nearly original form (including resources.arsc, classes.dex, 9.png. and XMLs)
2. Rebuilding decoded resources back to binary APK/JAR
3. Organizing and handling APKs that depend on framework resources
4. Smali Debugging (Removed in 2.1.0 in favor of IdeaSmali)
5. Helping with repetitive tasks

2.1.2 Requirements

The application requires only Java 1.7 (JRE 1.7) and some basic knowledge of Android SDK, AAPT and the Smali language alongside some in depth understanding of computer architecture, assembler and hexadecimal numbers.

2.1.3 Installation

The install process is very straight forward,

APPENDIX A

Begins an appendix

Bibliography

[1] OWASP, *Penetration testing methodologies*, 2015.