FACULTAD DE INGENIERIA

PROGRAMA DE ESPECIALIZACION EN SEGURIDAD DE LA INFORMACION

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACION

BOGOTÁ D.C.

AÑO DE ELABORACIÓN: 2020

TÍTULO

Verificación del grado de inseguridad de las infraestructuras Windows de Directorio Activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado.

AUTORES

Ardila Florez, Cristian David y Daza Castro, Juan Alberto

DIRECTOR(ES) / ASESOR(ES)

Jaimes Prada, Hector Dario y Osorio Reina, Diego

MODALIDAD: Software inteligente y Convergencia Tecnológica

PÁGINAS: 56 **TABLAS:** 8 **CUADROS:** N/A **FIGURAS:** 14 **ANEXOS:** 3

CONTENIDO

11. BIBLIOGRAFÍA

DESCRIPCIÓN

Este proyecto consiste en la verificación del grado de inseguridad de las infraestructuras Windows Server de Directorio Activo y construcción de una guía de aseguramiento, en un modelo de Directorio Activo On-Premise, la guía elaborada demostrará el grado de aseguramiento de dos entornos de Directorio Activo, uno inseguro y otro asegurado esto por medio de tres fases de PenTesting.

METODOLOGÍA

La elaboración de la guía de aseguramiento para Directorio Activo se plantea con base a la ejecución de tres fases de PenTesting White Box reconocimiento, escaneo y enumeración, que son las necesarias para alinear los objetivos de este proyecto, este PenTest tipo White Box implica que la evaluación de la seguridad y las pruebas son con conocimiento completo de la infraestructura, por parte del PenTester para este caso los autores del proyecto.

PALABRAS CLAVE

DIRECTORIO ACTIVO, PENTEST, VULNERABILIDAD, ASEGURAMIENTO, BUENAS PRACTICAS

CONCLUSIONES

Los resultados de la encuesta permitieron determinar el grado de aseguramiento de Directorios Activos reales y en producción, esta información se usa como apoyo para a la elaboración de la guía de aseguramiento.

Con el resultado de los entornos simulados se evidencio lo vulnerable que puede ser un Directorio Activo ante una configuración predeterminada de sistema operativo y de roles en Windows Server 2016.

Se puede contrastar el grado de exposición en los dos entornos de Directorio Activo de la guía de aseguramiento, donde se comprueba que la aplicación de buenas prácticas permite reducir las vulnerabilidades y grado de exposición ante atacantes. Las herramientas de PenTest permiten obtener información relevante a pesar de ser intrusivas, las ausencias de buenas prácticas permiten su ejecución sin ser detectadas.

Un Directorio Activo asegurado demanda un mayor tiempo del administrador de plataforma durante su implementación, configuración y gestión, esto debido a que se deben realizar más configuraciones en un entorno asegurado, con el fin de brindar apoyo y reducir tiempos, se proponen los scripts de automatización en la guía, esto optimiza tareas de rutina como por ejemplo la depuración de usuarios y la creación de Backups de GPO.

Es recomendable someter un Directorio Activo asegurado a análisis de PenTest periódicos, con el fin de fortalecer las configuraciones ya aplicadas.
Esta guía de aseguramiento de Directorio Activo deja abierta la posibilidad a futuras

investigaciones con diferentes entornos de Directorio Activo y pruebas PenTest.

FUENTES

389DS. (2017). 389 Directory Server. 389 Directory Server. https://directory.fedoraproject.org/

ADR Formacion. (2020). Definición de unidades organizativas en un servidor. https://www.adrformacion.com/knowledge/administracion-desistemas/definicion_de_unidades_organizativas_en_un_servidor.html

Apache Directory Studio. (2018). Apache Directory Studio. Apache Directory Studio. https://directory.apache.org/studio/

Beltran, S. (2019). Explotación avanzada del directorio activo. https://repository.ucatolica.edu.co/handle/10983/24059

Ceballos Lopez, A., Bautista Garcia, F., Mesa Guzman, L., & Argaez Quintero, C. (2020). Tendencias Cibercrimen Colombia 2019—2020. Policia Nacional. https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

CIS Controls. (2020). Cybersecurity Best Practices. https://www.cisecurity.org/cybersecurity-best-practices/

CVE - Search Results. (2020). CVE. http://cve.mitre.org/cgibin/cvekey.cgi?keyword=ldap

Deland-Han. (2020a). Active Directory FSMO. https://docs.microsoft.com/enus/troubleshoot/windows-server/identity/fsmo-roles

Deland-Han. (2020b). Usar RSoP. msc para recopilar la Directiva de equipo—Windows Server. https://docs.microsoft.com/es-es/troubleshoot/windowsserver/group-policy/use-resultant-set-of-policy-logging

Delprato, G. (2020). Windows Server 2012: Equipos de NIC (NIC Teaming).

WindowServer. https://windowserver.wordpress.com/2012/09/16/windows-server2012-equipos-de-nic-nic-teaming/

Dirk-jan. (2020). Ldapdomaindump [Python]. https://github.com/dirkjanm/ldapdomaindump (Original work published 2016)

Foulds, I. (2018). DNS y AD DS. https://docs.microsoft.com/es-es/windowsserver/identity/ad-ds/plan/dns-and-ad-ds

Franklin Smith, R. (2017). NIST Cybersecurity Framework for Active Directory Security. https://www.quest.com/whitepaper/nist-cybersecurity-framework-for-active-directory-security8132489/

Global server share by OS 2018-2019. (2018). Statista. https://www.statista.com/statistics/915085/global-server-share-by-os/

GNU Sistema Operativo. (2020). Free Software Foundation. https://www.gnu.org/home.es.html

GSuite. (2020). Google Form. https://gsuite.google.com/intl/es-419/products/forms/

IBM Security. (2020). IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/search/%23vulnerability

Icontec. (2020). Sistemas de Gestión de seguridad de la información. Icontec. https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-degestion-de-seguridad-de-la-informacion/

Introducción a Active Directory Domain Services. (2017). https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtualdc/active-directory-domain-services-overview

json.org. (2020). JSON. https://www.json.org/json-es.html

Lyon, G. (2020). Nmap: The Network Mapper—Free Security Scanner. https://nmap.org/

Metcalf, S. (2020a). ADSecurity. ADSecurity. https://adsecurity.org/

Metcalf, S. (2020b). TRIMARC Securing the Enterprise. Trimarc. https://www.trimarcsecurity.com/research

Microsoft. (2020a). Microsoft 365. https://www.microsoft.com/es-es/microsoft-365 Microsoft. (2020b). Net group. https://docs.microsoft.com/en-us/previousversions/windows/it-pro/windows-server-2012-r2-and-2012/cc754051(v=ws.11)

Microsoft. (2020c). Prueba Windows Server 2016 en Microsoft Evaluation Software [Windows Server]. Microsoft. https://www.microsoft.com/es-es/evalcenter/evaluatewindows-server-2016/

Microsoft. (2020d). Prueba Windows Server on-premises o en el cloud. Microsoft Cloud-Platform - ES (Español). https://www.microsoft.com/es-es/cloudplatform/windows-server-trial

MinTIC. (2018). Modelo de Seguridad. https://www.mintic.gov.co/gestionti/Seguridad-TI/Modelo-de-Seguridad/

Montemayor, D. (2020). Microsoft Security Compliance Toolkit 1.0—Windows security. https://docs.microsoft.com/en-us/windows/security/threatprotection/security-compliance-toolkit-10

Moore, S. (2018). Gartner Forecasts Worldwide Information Security Spending to

Exceed $124 Billion in 2019. https://www.gartner.com/en/newsroom/pressreleases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-toexceed-124-billion-in-2019

Moreno, J., Rodriguez, C., & Leguias, I. (2020). Revisión sobre propagación de ransomware en sistemas operativos Windows. I+D Tecnológico, 16(1), 39-45. https://doi.org/10.33412/idt.v16.1.2438

Neo4j. (2020). Neo4j Graph Platform. Neo4j Graph Database Platform. https://neo4j.com/

OffSec Services. (2020a). Kali. https://www.kali.org/

OffSec Services. (2020b). Polenum. https://tools.kali.org/password-attacks/polenum

OpenVAS. (2020). OpenVAS - Open Vulnerability Assessment Scanner. https://www.openvas.org/

Oracle. (2020). Oracle VM VirtualBox [Java]. https://www.virtualbox.org/
Ley 256 de 1996, (1996). http://www.secretariasenado.gov.co/senado/basedoc/ley_0256_1996.html

Poston, H. (2020). What are Black Box, Grey Box, and White Box Penetration Testing? Infosec Resources. https://resources.infosecinstitute.com/topic/what-areblack-box-grey-box-and-white-box-penetration-testing/

Rapid7. (2019). Under the Hoodie 2019 [Research, stories, and findings from Rapid7 penetration tests]. https://www.rapid7.com/research/under-the-hoodie/

Robbins, A. (2020). BloodHoundAD/BloodHound [PowerShell]. BloodHoundAD. https://github.com/BloodHoundAD/BloodHound (Original work published 2016)

Rodríguez Vallecilla, A., & Mina Loango, J. E. (2019). Descripción del funcionamiento de ataque del Malware ransomware (WannaCry) en sus procesos de infección, encriptación y propagación en el sistema operativo Windows [Thesis,

Universidad Santiago de Cali]. En Repositorio Institucional USC. https://repository.usc.edu.co/handle/20.500.12421/137

Ross, E. (2020). Gpresult. https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult

Ruef, M. (2020). Scipag/vulscan [Lua]. scip ag. https://github.com/scipag/vulscan (Original work published 2017)

SecurityFocus. (2020). SecurityFocus. https://www.securityfocus.com/

Seguridad Informatica. (2019). Penetration Testing. 20.

Tenable. (2020). Nessus.

https://www.tenable.com/downloads/nessus?loginAttempted=true

Tridgell, A. (2020). net—Tool for administration of Samba and remote CIFS servers. https://www.samba.org/samba/docs/current/man-html/net.8.html

Normativa Nacional, Ley 1266 de 2008, (2008). https://ucatolica.codigosleyex.info/LyxNormas/view/15709/htm

Normativa Nacional, Ley 1273 de 2009, (2009). https://ucatolica.codigosleyex.info/LyxNormas/view/9282/htm

Normativa Nacional, Ley 1581 de 2012, (2012). https://ucatolica.codigosleyex.info/LyxNormas/view/21817/htm

Universidad Católica. (2020). UCatolica. Universidad Católica De Colombia. https://www.ucatolica.edu.co/portal/

Vazarkar, R. (2020). BloodHoundAD/SharpHound [C#]. BloodHoundAD. https://github.com/BloodHoundAD/SharpHound (Original work published 2017)

Why Active Directory (AD) Protection Matters. (2020). https://www.bankinfosecurity.com/whitepapers/active-directory-ad-protectionmatters-w-5783

LISTA DE ANEXOS

ANEXO A
Articulo IEEE verificación del grado de inseguridad de las infraestructuras Windows de Directorio Activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado en el ambiente simulado.

ANEXO B
Guía de Aseguramiento de Directorio Activo, documento de análisis previo y posterior al aseguramiento del Directorio Activo de Windows Server 2016.

ANEXO C
Resultados de encuesta de Aseguramiento de Directorio Activo, para la elaboración de la guía de aseguramiento de Directorio Activo.