UÍDE
Universidad Internacional del Ecuador

UNIVERSIDAD NEBRIJA

UÍDE Open

MAESTRÍA EN CIBERSEGURIDAD

PLAN DEL PROYECTO DE INVESTIGACIÓN

TÍTULO: "METODOLOGÍA PARA EL PROCESO DE PENTESTING Y ESCALADO DE PRIVILEGIOS EN ENTORNOS EMPRESARIALES MEDIANTE LA EXPLOTACIÓN DE KERBEROS ASOCIADO AL DIRECTORIO ACTIVO"

Alumno: Cristian Andrés Pazmiño Gómez

Tutor: Ramiro Alejandro Castillo Oleas

Quito, febrero de 2021

RESUMEN

El presente trabajo de investigación tiene por objeto desarrollar una metodología para la ejecución de pruebas avanzadas de auditoria ofensiva, ataques dirigidos y explotación de vulnerabilidades en el proceso de autenticación utilizado por Kerberos, debido a que su rol para la administración de recursos, la gestión y control de acceso de los usuarios, cumplen con una tarea fundamental y de relevancia dentro de la Organización, es por ello que surge la necesidad de entender su funcionamiento mediante la realización de pruebas de auditoria ofensiva sobre los procesos de autenticación propios del protocolo Kerberos, a fin de identificar vulnerabilidades que pongan en riesgo la integridad y confidencialidad de los usuarios que forman parte del directorio activo.

La metodología describe una sucesión de procesos y técnicas enfocadas desde dos aristas puntuales al ejecutar una auditoria de seguridad ofensiva en entornos empresariales, un usuario sin credenciales y, por otra parte, un usuario con credenciales válidas y asociado al directorio activo con permisos básicos-limitados. Una vez aplicada la metodología se obtuvo como resultado un escalamiento de privilegios, convirtiendo a los dos tipos de usuarios objeto de pruebas en “NT Authority \ System” o también conocido como “Administrador de dominio”. Al comprometer una cuenta de Administrador, se expone a toda la organización a un riesgo muy alto, por cuanto este tipo de cuentas tienen acceso a todos los recursos administrados por el dominio, control sobre todos los usuarios, servidores, estaciones de trabajo y a los datos.

Una vez obtenidos los resultados de la ejecución y aplicación de la metodología de auditoria ofensiva sobre los procesos de autenticación del protocolo Kerberos, se estructuró un documento con recomendaciones dirigidas a los administradores de dominio, a fin de que puedan subsanar y tomar acciones que mitiguen el riesgo asociado a la explotación del protocolo Kerberos en entornos empresariales.

PALABRAS CLAVE

Kerberos, Pentesting, ActiveDirectory, Impacket, DomainAdmin, privEsc, Mimikatz, Kerbrute, psExec, ASREProast, Kerberoasting, PTK, PTT, Zerologon.

ABSTRACT

The objective of this research work was to develop a methodology for the execution of advanced offensive audit tests, targeted attacks and exploitation of vulnerabilities in the authentication process used by Kerberos, due to the fact that its role for the administration of resources, management and access control of users, It is for this reason that the need arises to understand its operation by performing offensive audit tests on the authentication processes of the Kerberos protocol, in order to identify vulnerabilities that may compromise the integrity and confidentiality of the users that are part of the active directory.

The methodology describes a succession of processes and techniques focused on two specific aspects in the execution of an offensive security audit in business environments, a user without credentials and, a user with valid credentials and associated to the active directory with basic-limited permissions. Once the methodology was applied, a privilege escalation was obtained as a result, converting the two types of users under test into "NT Authority System" or also known as "Domain Administrator". By compromising an Administrator account, the entire organization is exposed to a very high risk, since this type of account has access to all the resources managed by the domain, control over all users, servers, workstations and data.

Based on the results obtained from the execution and application of the offensive audit methodology on the authentication processes of the Kerberos protocol, a document was structured with recommendations for domain administrators, so that they can remedy and take actions to mitigate the risk associated with the exploitation of the Kerberos protocol in enterprise environments.

KEYWORDS

Kerberos, Pentesting, ActiveDirectory, Impacket, DomainAdmin, privEsc, Mimikatz, Kerbrute, psExec, ASREProast, Kerberoasting, PTK, PTT, Zerologon.