



# UNITEC<sup>MR</sup>

Universidad Tecnológica de México

## MAESTRÍA EN SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN

### HACKING ÉTICO Y ANÁLISIS FORENSE

2023-03

CAMPUS SUR

PROFESOR MAESTRO RODRÍGUEZ AGUILAR BENITO ALAN

ENTREGABLE FINAL: “PROPUESTA DE REPORTE DE HACKEO  
ÉTICO Y DE CÓMPUTO FORENSE”

ALUMNA KUHLLIGER MARTÍNEZ MARTHA GUADALUPE

NÚMERO DE CUENTA: 334011227

30 DE JULIO DEL 2023

## TABLA DE CONTENIDO

<b>ÍNDICE DE FIGURAS.....</b>	<b>5</b>
<b>ÍNDICE DE TABLAS.....</b>	<b>9</b>
<b>RESUMEN .....</b>	<b>10</b>
<b>ABSTRACT.....</b>	<b>11</b>
<b>CAPÍTULO I: METODOLOGÍA APLICADA .....</b>	<b>12</b>
<b>Herramientas de Hacking Ético .....</b>	<b>12</b>
<b>VMware Workstation 16 Player .....</b>	<b>12</b>
<b>Kali Linux versión 2023.2 .....</b>	<b>12</b>
<b>Metasploitable versión 2.....</b>	<b>13</b>
<b>OWASP Risk Rating Calculator.....</b>	<b>14</b>
<b>Plataformas de búsqueda de vulnerabilidades .....</b>	<b>15</b>
<b>MITRE ATT&amp;CK .....</b>	<b>15</b>
<b>National Vulnerability Database (NVD) .....</b>	<b>16</b>
<b>Exploit Database .....</b>	<b>17</b>
<b>CVE .....</b>	<b>18</b>
<b>Herramientas de Computación Forense .....</b>	<b>19</b>
<b>AccessData FTK Imager versión 4.7.1.....</b>	<b>19</b>
<b>AccessData Registry Viewer versión 1.8.0.5 .....</b>	<b>20</b>
<b>Index.dat Analyzer versión 2.5 .....</b>	<b>21</b>
<b>CAPÍTULO II: ESTUDIO DE LA ORGANIZACIÓN .....</b>	<b>23</b>
<b>Historia.....</b>	<b>23</b>
<b>Misión .....</b>	<b>23</b>
<b>Visión.....</b>	<b>23</b>
<b>Descripción de las actividades principales de la organización .....</b>	<b>23</b>
<b>Organigrama .....</b>	<b>23</b>
<b>CAPÍTULO III: EVIDENCIA DE LA IDENTIFICACIÓN Y EXPLOTACIÓN DE CINCO VULNERABILIDADES .....</b>	<b>26</b>
<b>Vulnerabilidad 1: SSH Login Check Scanner .....</b>	<b>32</b>
<b>Vulnerabilidad 2: Apple Remote Desktop Root Vulnerability .....</b>	<b>36</b>
<b>Vulnerabilidad 3: TCP Port Scanner.....</b>	<b>40</b>
<b>Vulnerabilidad 4: Samba Username map script .....</b>	<b>44</b>
<b>Vulnerabilidad 5: UnrealIRCd 3.2.8.1 Backdoor Command Execution .....</b>	<b>47</b>

<b>CAPÍTULO IV: ANÁLISIS DE VULNERABILIDADES.....</b>	<b>51</b>
OWASP Risk Rating Calculator.....	51
Vulnerabilidad CVE-1999-0502.....	51
Vulnerabilidad CVE-2017-13872.....	52
Vulnerabilidad CVE-2002-2179.....	53
Vulnerabilidad CVE-2007-2447.....	54
Vulnerabilidad CVE-2010-2075.....	54
Matriz de Riesgos.....	55
<b>CAPÍTULO V: ANÁLISIS FORENSE.....</b>	<b>59</b>
¿Cuál es la dirección IP del equipo de cómputo de origen?.....	64
¿Qué usuarios tiene configurados en el equipo de cómputo original? .....	68
¿Cuándo fue la última vez que se autentificaron en el equipo? .....	69
¿Cuál es el número de serie del disco duro? .....	73
¿Cuáles fueron los últimos sitios que se visitaron en el equipo de cómputo?.....	74
¿Existen archivos eliminados en la evidencia del equipo de cómputo?.....	83
¿Quién eliminó los archivos? .....	84
¿Qué contenían los archivos que fueron eliminados? .....	84
¿Cuáles eran los nombres y ubicaciones originales de los archivos eliminados? .....	86
¿Existen mensajes de correo electrónico relacionados con el fraude nigeriano?.....	87
En caso de ser positiva la respuesta anterior ¿Quién y cuándo se envió? .....	92
<b>CAPÍTULO VI: DESCRIPCIÓN DE LA PROPUESTA.....</b>	<b>94</b>
<b>CAPÍTULO VI: SOLUCIONES Y RECOMENDACIONES.....</b>	<b>95</b>
Medidas de seguridad para corregir vulnerabilidades.....	95
Vulnerabilidad 01 – SSH Login Check Scanner – CVE-1999-0502. ....	95
Vulnerabilidad 02 – Apache Remote Desktop Root Vulnerability – CVE-2017-13872.....	95
Vulnerabilidad 03 – TCP Port Scanner – CVE-2002-2179.....	96
Vulnerabilidad 04 – Samba Username map script – CVE-2007-2447.....	96
Vulnerabilidad 05 – UnrealIRCd 3.2.8.1 Backdoor Command Execution – CVE.2010-2075....	96
Recomendaciones de seguridad para equipos sometidos a análisis .....	96
<b>CAPÍTULO VII: DISCUSIÓN DE RESULTADOS Y CONCLUSIONES .....</b>	<b>97</b>
<b>BIBLIOGRAFÍA .....</b>	<b>98</b>



## ÍNDICE DE FIGURAS

Figura 1. VMware Workstation 16 Player. ....	12
Figura 2. Kali Linux 2023.2. ....	13
Figura 3. Metasploitable 2. ....	14
Figura 4. OWASP Risk Rating Calculator. ....	15
Figura 5. MITRE ATT&CK. ....	16
Figura 6. National Vulnerability Database. ....	17
Figura 7. Exploit Database. ....	18
Figura 8. CVE. ....	19
Figura 9. FTK Imager. ....	20
Figura 10. Registry Viewer. ....	21
Figura 11. Index.dat Analyzer. ....	22
Figura 12. Organigrama de R&K Audit. ....	24
Figura 13. Máquinas Virtuales. ....	26
Figura 14. Máquina virtual Metasploitable 2. ....	26
Figura 15. Dirección IP de Metasploitable. ....	27
Figura 16. Dirección IP en navegador. ....	27
Figura 17. Ejecutando máquina virtual Kali. ....	28
Figura 18. Máquina virtual de Kali. ....	28
Figura 19. Comando ping. ....	29
Figura 20. Comando nmap -sV IP. ....	29
Figura 21. Comando nmap -O IP. ....	30
Figura 22. Comando nmap -A IP. ....	30
Figura 23. Metasploit framework. ....	31
Figura 24. Inicio de Metasploit Framework. ....	31
Figura 25. Comando sudo msfdb init && msfconsole. ....	32
Figura 26. Comando search ssh. ....	33
Figura 27. Comando use auxiliary/scanner/ssh/ssh_login. ....	33
Figura 28. Comando show options SSH Login. ....	34
Figura 29. Ingresar datos para SSH Login. ....	34
Figura 30. Verificar valores SSH Login. ....	35
Figura 31. Comando show info a SSH Login. ....	35
Figura 32. Exploit SSH Login. ....	36
Figura 33. Comando search vnc. ....	37
Figura 34. Comando use auxiliary/scanner/vnc/ard_root_pw. ....	37
Figura 35. Comando show options vnc. ....	38
Figura 36. Ingresar RHOST. ....	38
Figura 37. Verificar valor RHOST vnc. ....	39
Figura 38. Comando show info vnc. ....	39
Figura 39. Exploit vnc. ....	40
Figura 40. Comando search portscan tcp. ....	40
Figura 41. Comando use auxiliary/scanner/portscan/tcp. ....	41
Figura 42. Comando show options TCP. ....	41
Figura 43. Comando llenar campos TCP. ....	41

Figura 44. Verificar campos TCP.....	42
Figura 45. Comando show info TCP. ....	42
Figura 46. Exploit TCP. ....	43
Figura 47. db_nmap -sV -p Ports IP.....	43
Figura 48. Comando search samba. ....	44
Figura 49. Comando use exploit/multi/samba/usermap_script. ....	44
Figura 50. Comando show options Samba. ....	45
Figura 51. Ingresar valores a RHOST y LHOST.....	45
Figura 52. Verificar valores Samba. ....	46
Figura 53. Comando show info Samba.....	46
Figura 54. Exploit Samba. ....	47
Figura 55. Comando search ircd 3281. ....	47
Figura 56. Comando use exploit/unix/irc/unreal_ircd_3281_backdoor. ....	48
Figura 57. Comando show options ircd.....	48
Figura 58. Comando show payloads.....	48
Figura 59. Llenar campos ircd.....	49
Figura 60. Verificar datos ircd.....	49
Figura 61. Comando show info ircd.....	50
Figura 62. Exploit ircd. ....	50
Figura 63. OWASP Calculator CVE-1999-0502.....	52
Figura 64. OWASP Calculator CVE-2017-13872.....	53
Figura 65. OWASP Calculator CVE-2002-2179.....	53
Figura 66. OWASP Calculator CVE-2007-2447.....	54
Figura 67. OWASP Calculator CVE-2010-2075.....	55
Figura 68. Matriz de riesgos. ....	58
Figura 69. Ejecutando FTK Imager. ....	59
Figura 70. Agregar imagen forense. ....	60
Figura 71. Tipo de evidencia.....	60
Figura 72. Ruta de origen de imagen forense. ....	60
Figura 73. Importar imagen forense.....	61
Figura 74. Ruta de origen establecida. ....	61
Figura 75. Imagen forense cargada. ....	61
Figura 76. Ruta MANTOOTH/root/Windows/System32/config. ....	62
Figura 77. Exportar archivos config. ....	63
Figura 78. Resultado de exportar archivos config. ....	63
Figura 79. Archivos config en Documentos. ....	64
Figura 80. Archivo SYSTEM.....	64
Figura 81. Guía de la ruta para IP.....	65
Figura 82. Dirección IP de evidencia digital.....	65
Figura 83. Exportar Hash de archivo SYSTEM.....	66
Figura 84. Ruta de destino de archivo Hash de SYSTEM. ....	66
Figura 85. Archivo Hash de SYSTEM descargado.....	67
Figura 86. Archivo Hash de System en Excel. ....	67
Figura 87. Archivo SAM. ....	68

Figura 88. Guía para ruta de usuarios. ....	68
Figura 89. Ruta de nombres de usuarios.....	69
Figura 90. Guía de ruta última sesión.....	70
Figura 91. Inicio de sesión de Administrator. ....	70
Figura 92. Inicio de sesión de Guest.....	71
Figura 93. Inicio de sesión de Wes Mantooth.....	71
Figura 94. Inicio de sesión de Dracula.....	72
Figura 95. Inicio de sesión de Laurent.....	72
Figura 96. Número de Serie.....	73
Figura 97. Archivo txt de imagen forense.....	73
Figura 98. Número de serie del disco.....	74
Figura 99. Exportar valores Hash de la imagen forense. ....	75
Figura 100. Ruta de destino.....	75
Figura 101. Archivo Hash.....	76
Figura 102. Buscador de Excel.....	76
Figura 103. Ruta de archivo index.dat.....	77
Figura 104. Exportar archivo index.dat. ....	77
Figura 105. Mensaje de exportación exitosa.....	78
Figura 106. Ejecutando Index.dat Analyzer. ....	78
Figura 107. Seleccionar ruta de origen.....	79
Figura 108. Buscar archivo index.dat. ....	79
Figura 109. Mensaje archivo agregado. ....	79
Figura 110. Búsqueda de la ruta de origen. ....	80
Figura 111. Historial de Internet Explorer completo.....	80
Figura 112. Guardar historial.....	81
Figura 113. Historial de sistios web guardado.....	81
Figura 114. Visualización del historial de Internet. ....	82
Figura 115. Buscar ruta de Firefox.....	82
Figura 116. Historial de Firefox.....	83
Figura 117. Archivos en papelera de reciclaje.....	83
Figura 118. Usuario que eliminó los archivos.....	84
Figura 119. Archivos eliminados.....	85
Figura 120. Imágenes eliminadas. ....	85
Figura 121. Archivo de texto y de Java eliminados.....	86
Figura 122. Ruta y nombre original. ....	87
Figura 123. Ruta de correos Outlook.....	88
Figura 124. Exportar correos de Outlook.....	88
Figura 125. Ruta de destino para los correos. ....	89
Figura 126. Archivo de Outlook exportado exitosamente. ....	89
Figura 127. Aplicación de Outlook. ....	90
Figura 128. Botón para importar archivo pst. ....	90
Figura 129. Importar archivo.....	91
Figura 130. Archivo de Outlook.....	91
Figura 131. Ruta de destino de archivo de Outlook.....	91

Figura 132. Indicar carpeta para importar.....	92
Figura 133. Archivo de Outlook importado a otra cuenta.....	92
Figura 134. Fraude nigeriano.....	93
Figura 135. Propuesta para mejorar seguridad.....	94



## ÍNDICE DE TABLAS

Tabla 1. Catálogo de vulnerabilidades.....	51
Tabla 2. Tabla de probabilidad.....	55
Tabla 3. Tabla de Impacto.....	56
Tabla 4. Tabla de criterios de riesgo. ....	56
Tabla 5. Tabla de principios de seguridad. ....	56
Tabla 6. Tabla de identificación de vulnerabilidades.....	57
Tabla 7. Tabla de nivel de riesgo.....	57
Tabla 8. Registro de inicio de sesión.....	69
Tabla 9. Historial de Internet Explorer.....	74
Tabla 10. Nombres y ubicaciones originales de los archivos.....	86
Tabla 11. Catálogo de vulnerabilidades definido.....	95

## RESUMEN

El presente documento permitió reforzar y poner en práctica los conceptos que se aprendieron en el curso de Hacking Ético y Análisis Forense mediante el desarrollo de una propuesta que dará solución a una problemática y mejorará la seguridad de una organización, la cual se llamará R&K Audit para este caso de estudio.

Este caso de estudio consistió en detectar vulnerabilidades a través de pruebas de penetración aplicando conocimientos y principios de Hacking Ético, con el propósito de proteger a la organización y guiarla para detectar sus vulnerabilidades y prevenir ataques dañinos causados por los ciberdelincuentes.

Se realizó una investigación sobre herramientas que se implementaron, así como las plataformas de búsqueda de vulnerabilidades, se instaló el sistema operativo Kali Linux y la máquina virtual Metasploitable 2, se ejecutaron pruebas de penetración para detectar vulnerabilidades, se desarrolló un análisis de vulnerabilidades para calcular el impacto y la probabilidad con la ayuda de aplicación OWASP Risk Rating Calculator y se desarrolló una matriz de riesgos. Además, se analizó una imagen forense, donde se obtuvo la dirección IP del equipo, el nombre de los usuarios y la última vez que iniciaron sesión, el número de serie del disco duro, el historial de Internet Explorer, el nombre y la ubicación de los archivos enviados a la papelería de reciclaje y los correos electrónicos de una cuenta de Outlook.

Con base a lo mencionado anterior se desarrolló una propuesta que garantizará una mayor seguridad en los sistemas y equipos informáticos de la organización R&K Audit. También se describen soluciones y recomendaciones para corregir las vulnerabilidades que se detectaron en los sistemas del Departamento de Asesoría en Riesgo.

Por confidencialidad se ha modificado el nombre de la organización R&K Audit.

## ABSTRACT

**This document allowed to reinforce and put into practice the concepts learned in the course of *Ethical Hacking and Forensic Analysis* through the development of a proposal that will provide a solution to a problem and improve the security of an organization, which will be called *R&K Audit* for this case study.**

**This case study consisted of detecting vulnerabilities through penetration testing by applying knowledge and principles of Ethical Hacking, in order to protect the organization and guide it to detect its vulnerabilities and prevent harmful attacks caused by cybercriminals.**

**An investigation was conducted on tools that were implemented, as well as vulnerability search platforms, the Kali Linux operating system and the Metasploitable 2 virtual machine were installed, penetration tests were executed to detect vulnerabilities, a vulnerability analysis was developed to calculate the impact and probability with the help of OWASP Risk Rating Calculator application and a risk matrix was developed. In addition, a forensic image was analyzed, where the IP address of the computer, the name of the users and the last time they logged in, the serial number of the hard disk, the history of Internet Explorer, the name and location of the files sent to the recycle bin and the e-mails from an Outlook account were obtained.**

**Based on, a proposal was developed to ensure greater security in the computer systems and equipment of the R&K Audit organization. It also describes solutions and recommendations to correct the vulnerabilities detected in the systems of the Risk Advisory Department.**

**For confidentiality reasons, the name of the R&K Audit organization has been changed.**