

# Attacking & Securing CI/CD Pipelines



Figure 1



# Table of Contents

<b>TABLE OF CONTENTS</b> .....	<b>1</b>
<b>INTRODUCTION</b> .....	<b>7</b>
<b>ABOUT THE ATTACKING AND SECURING CI/CD PIPELINES (ASCPC) CERTIFICATION COURSE</b> .....	<b>7</b>
<b>COURSE APPROACH</b> .....	<b>7</b>
<b>COURSE SUPPORT</b> .....	<b>8</b>
<b>LAB INSTRUCTIONS</b> .....	<b>9</b>
<b>REQUIRED HARDWARE</b> .....	<b>9</b>
<b>REQUIRED ACCOUNTS</b> .....	<b>9</b>
<b>REQUIRED SOFTWARE</b> .....	<b>9</b>
<b>CREATE GITHUB ACCOUNT</b> .....	<b>9</b>
<b>CREATE CIRCLECI ACCOUNT</b> .....	<b>10</b>
<b>CREATE AWS ACCOUNT</b> .....	<b>10</b>
<b>AZURE ACCOUNT AND SETUP</b> .....	<b>11</b>
<b>INSTALLING GIT CLI</b> .....	<b>12</b>
<b>INSTALLING DOCKER</b> .....	<b>12</b>
<b>INSTALLING NPM CLI</b> .....	<b>12</b>
<b>INSTALLING KUBECTL CLI</b> .....	<b>13</b>
<b>INSTALLING AZURE CLI</b> .....	<b>13</b>
<b>1 CI/CD ATTACK SIMULATION LAB SETUP</b> .....	<b>14</b>
<b>LAB OVERVIEW</b> .....	<b>14</b>
1.1.1 LOGGING INTO PORTAL.AZURE.COM AND COLLECTING CI/CD APP CREDENTIALS .....	14
1.1.2 CONFIGURING AZURE DEVOPS FOR WKLCICD.AZUREWEBSITES.NET .....	21
1.1.3 GITHUB INFORMATION TO SHARE IN PORTAL .....	25
<b>2 LAB - EXPLOIT GITHUB INSECURE CONTEXTS</b> .....	<b>28</b>
<b>LAB OVERVIEW</b> .....	<b>28</b>
<b>HANDS ON: EXPLOIT INSECURE CONTEXT</b> .....	<b>28</b>
2.1.1 FORK THE LAB REPOSITORY FOR THIS LAB .....	28
2.1.2 CLONE THE REPOSITORY LOCALLY .....	29
2.1.3 EXAMINE THE GITHUB ACTIONS FILE .....	30
2.1.4 CREATE BRANCH WITH A MALICIOUS PAYLOAD .....	31
2.1.5 CREATE AND MODIFY THE MALICIOUS BRANCH .....	31
2.1.6 ENABLING THE GITHUB ACTIONS WORKFLOW .....	33



2.1.7 CREATE A NEW PULL REQUEST .....	34
2.1.8 SWITCH TO MAIN BRANCH, MERGE THE PAYLOAD, AND CONTRIBUTE .....	36
2.1.9 INSPECT WORKFLOW OUTPUT .....	38
2.1.10 RESET AND CLEANUP ENVIRONMENT .....	40
<b>HANDS ON: SANITIZE DATA TO MITIGATE CONTEXT INJECTION .....</b>	<b>40</b>
2.1.11 CREATE BRANCH WITH A MALICIOUS PAYLOAD .....	41
2.1.12 EXAMINE THE GITHUB ACTIONS FILE .....	41
2.1.13 SWAP WORKFLOW FILES AND PUSH CHANGES TO GITHUB .....	41
2.1.14 CREATE A NEW PULL REQUEST TO MERGE BRANCH INTO MAIN .....	42
2.1.15 INSPECT MITIGATION WORKFLOW OUTPUT .....	42
2.1.16 REMOVE LOCAL GIT REPOSITORY AND FORKED REPOSITORY IN GITHUB .....	43
<b>CONCLUSION .....</b>	<b>44</b>

### **3 LAB - EXPLOIT GITHUB PULL REQUEST TARGET..... 45**

<b>LAB OVERVIEW .....</b>	<b>45</b>
<b>HANDS ON: EXPLOIT PULL REQUEST TARGETS .....</b>	<b>45</b>
3.1.1 FORK THE LAB REPOSITORY FOR THIS LAB .....	45
3.1.2 CLONE THE REPOSITORY LOCALLY .....	46
3.1.3 EXAMINE THE GITHUB ACTIONS FILE .....	47
3.1.4 EXAMINE THE CURRENT PACKAGE.JSON .....	48
3.1.5 ENABLING THE GITHUB ACTIONS WORKFLOW .....	49
3.1.6 REPLACE THE PACKAGE.JSON WITH THE MALICIOUS VERSION AND PUSH CHANGES .....	49
3.1.7 CREATE A PULL REQUEST .....	53
3.1.8 INSPECT THE WORKFLOW .....	55
<b>HANDS ON: REQUIRE APPROVALS FOR ACTIONS .....</b>	<b>57</b>
3.1.9 REQUIRE APPROVAL FOR ALL EXTERNAL CONTRIBUTORS .....	57
3.1.10 HANDS ON: RESTRICT WORKFLOW PERMISSIONS .....	59
3.1.11 REMOVE LOCAL GIT REPOSITORY AND FORKED REPOSITORY IN GITHUB .....	59
<b>CONCLUSION .....</b>	<b>60</b>

### **4 LAB - GITHUB ISSUE COMMENT INJECTION..... 61**

<b>LAB OVERVIEW .....</b>	<b>61</b>
<b>HANDS ON: EXPLOIT ISSUE COMMENT INJECTION .....</b>	<b>61</b>
4.1.1 CLONE THE REPOSITORY LOCALLY .....	61
4.1.2 EXAMINE THE VULNERABLE GITHUB ACTIONS FILE .....	61
4.1.3 CREATE A NEW ISSUE .....	62
4.1.4 ADD A MALICIOUS COMMENT TO THE ISSUE .....	65
4.1.5 INSPECT WORKFLOW OUTPUT .....	65
<b>HANDS ON: SANITIZE DATA TO MITIGATE COMMENT INJECTION .....</b>	<b>67</b>
4.1.6 EXAMINE A GITHUB ACTIONS FILE THAT MITIGATES THIS ISSUE .....	67
4.1.7 SWAP WORKFLOW FILES AND PUSH CHANGES TO GITHUB .....	68
4.1.8 ADD ANOTHER MALICIOUS COMMENT .....	69
4.1.9 INSPECT MITIGATION WORKFLOW OUTPUT .....	69



4.1.10 REMOVE LOCAL GIT REPOSITORY AND FORKED REPOSITORY IN GITHUB..... 70  
CONCLUSION..... 71

**5 LAB - GITHUB WORKFLOW RUN EXPLOIT ..... 72**

LAB OVERVIEW ..... 72  
HANDS ON: EXPLOIT WORKFLOW\_RUN MISCONFIGURATIONS..... 72  
5.1.1 FORK THE LAB REPOSITORY FOR THIS LAB ..... 72  
5.1.2 CLONE THE REPOSITORY LOCALLY..... 73  
5.1.3 EXAMINE THE VULNERABLE GITHUB ACTIONS WORKFLOW FILES..... 74  
5.1.4 EXAMINE CURRENT PACKAGE.JSON FILE ..... 76  
5.1.5 EXAMINE THE MALICIOUS PACKAGE.JSON..... 77  
5.1.6 CREATE A NEW BRANCH..... 78  
5.1.7 SWAP IN MALICIOUS PACKAGE.JSON AND PUSH CHANGES TO GITHUB ..... 78  
5.1.8 CREATE A PULL REQUEST TO MERGE EXPLOIT-BRANCH INTO MAIN BRANCH ..... 79  
5.1.9 INSPECT WORKFLOW OUTPUT..... 81  
5.1.10 REMOVE LOCAL GIT REPOSITORY AND FORKED REPOSITORY IN GITHUB..... 83  
CONCLUSION..... 85

**6 LAB - BYPASSING GITHUB PROTECTED BRANCHES..... 86**

LAB OVERVIEW ..... 86  
HANDS ON: BYPASS PROTECTED BRANCH ..... 86  
6.1.1 EXAMINE THE VULNERABLE GITHUB ACTIONS WORKFLOW FILE..... 86  
6.1.2 EXPLOITING THE WORKFLOW: CREATE MALICIOUS PULL REQUEST ..... 89  
6.1.3 TRIGGERING THE AUTO-MERGE VIA MALICIOUS PULL REQUEST TITLE..... 90  
6.1.4 REMOVE LOCAL GIT REPOSITORY AND FORKED REPOSITORY IN GITHUB..... 92  
CONCLUSION..... 92

**7 LAB - SETTING UP A CIRCLECI PIPELINE..... 93**

LAB OVERVIEW ..... 93  
HANDS ON: SETTING UP CIRCLECI PIPELINE..... 93  
7.1.1 LOGIN TO CIRCLECI AND CREATE ORGANIZATION ..... 93  
7.1.2 CREATE A PROJECT ..... 94  
7.1.3 CREATE A PIPELINE ..... 95  
7.1.4 CONNECT GITHUB ACCOUNT TO PIPELINE ..... 96  
7.1.5 PICK REPOSITORY TO USE FOR PIPELINE ..... 99  
7.1.6 SET UP CONFIG..... 100  
7.1.7 SET UP TRIGGER..... 100  
7.1.8 TEST THE PIPELINE ..... 102

**8 LAB - ABUSING A CIRCLECI API TOKEN ..... 103**



<b>LAB OVERVIEW:</b> .....	<b>103</b>
8.1.1 ENUMERATION OF THE TOKEN .....	103
8.1.2 IDENTIFY TOKEN SCOPE AND ASSOCIATED ORGANIZATIONS.....	104
8.1.3 ENUMERATING PROJECTS USING THE ORGANIZATION ID .....	105
8.1.4 DEEP DIVE INTO CIRCLECI METADATA ENUMERATION .....	106
8.1.5 HUNTING FOR ARTIFACTS IN CIRCLECI BUILD OUTPUT .....	111
8.1.6 CONCLUSION .....	113

**9 LAB - SETTING UP A CI/CD PIPELINE IN AZURE WITH DOCKER CONTAINER..... 114**

<b>LAB OVERVIEW</b> .....	<b>114</b>
<b>HANDS ON: CREATE CI/CD PIPELINE</b> .....	<b>114</b>
9.1.1 FORK THE LAB REPOSITORY FOR THIS LAB .....	114
9.1.2 CLONE THE REPOSITORY LOCALLY.....	115
9.1.3 EXAMINE THE GITHUB ACTIONS WORKFLOW FILE .....	115
9.1.4 CREATE AN AZURE CONTAINER REGISTRY.....	117
9.1.5 CREATE ACR ACCESS TOKEN .....	119
9.1.6 SET GITHUB ACR SECRETS .....	122
9.1.7 CREATE AZURE APP SERVICE .....	123
9.1.8 TRIGGER WORKFLOW TO RUN.....	128
9.1.9 INSPECT WORKFLOW OUTPUT.....	129
9.1.10 VIEW RUNNING NODEJS APP IN APP SERVICE .....	130
<b>CONCLUSION</b> .....	<b>132</b>

**10 LAB - EXPLOITING OVERPRIVILEGED CI/CD SERVICE ACCOUNTS IN KUBERNETES ..... 133**

<b>LAB OVERVIEW</b> .....	<b>133</b>
<b>HANDS ON: EXPLOIT OVERPRIVILEGED SERVICE ACCOUNTS</b> .....	<b>133</b>
10.1.1 FORK THE LAB REPOSITORY FOR THIS LAB .....	133
10.1.2 CLONE THE REPOSITORY LOCALLY.....	134
10.1.3 CREATE A KUBERNETES CLUSTER IN AZURE .....	134
10.1.4 AUTHENTICATE TO AZURE VIA AZURE CLI.....	140
10.1.5 AUTHENTICATE WITH OUR AZURE KUBERNETES CLUSTER VIA CLI .....	141
10.1.6 CREATE KUBERNETES PODS.....	142
10.1.7 CREATE A CONTAINER REGISTRY .....	144
10.1.8 UPDATE LOCAL DEPLOYMENT MANIFEST FILE .....	146
10.1.9 SETUP A KUBERNETES AUTOMATED APPLICATION DEPLOYMENT.....	147
10.1.10 REVIEW OUTPUT OF NEW AUTOMATED GITHUB ACTIONS WORKFLOW .....	157
10.1.11 VIEW RUNNING APPLICATION IN BROWSER .....	158
10.1.12 SET UP AN ATTACK SCENARIO .....	160
10.1.13 EXPLOIT THE NEWLY EXPOSED PATH .....	161
<b>CONCLUSION</b> .....	<b>166</b>

**11 LAB - CI/CD SUPPLY CHAIN ATTACK IN THIRD PARTY LIBRARIES..... 167**



<b>LAB OVERVIEW</b> .....	<b>167</b>
<b>HANDS ON: SIMULATE SUPPLY CHAIN ATTACK</b> .....	<b>167</b>
11.1.1 CONTINUE USING REPOSITORY FROM THE PREVIOUS LAB .....	167
11.1.2 INSTALL THIRD-PARTY LIBRARY INTO APPLICATION.....	167
11.1.3 INTEGRATE THIRD-PARTY LIBRARY INTO APPLICATION.....	167
11.1.4 VIEW UPDATED APP IN BROWSER .....	169
11.1.5 UPDATE THIRD-PARTY LIBRARY VERSION .....	170
11.1.6 VIEW UPDATED APP IN BROWSER .....	171
<b>CONCLUSION</b> .....	<b>172</b>

**12 LAB - HOSTING AN APPLICATION WITH HELM..... 173**

<b>LAB OVERVIEW</b> .....	<b>173</b>
<b>HANDS ON: EXPLOIT OVERPRIVILEGED SERVICE ACCOUNTS</b> .....	<b>173</b>
12.1.1 SETTING UP HELM CHARTS .....	173
12.1.2 RUNNING THE HELM CHARTS .....	175
12.1.3 UPGRADING THE HELM APP .....	176
<b>CONCLUSION</b> .....	<b>177</b>

**13 LAB - ACCESSING AZURE DEVOPS VIA FUNCTION APP MANAGED IDENTITY..... 178**

<b>LAB OVERVIEW</b> .....	<b>178</b>
<b>HANDS ON: ABUSING MANAGED IDENTITY</b> .....	<b>178</b>
13.1.1 USING THE STARTING POINT URL LET'S VISIT THE WEBSITE .....	178
13.1.2 ENUMERATE THE ORGANIZATION.....	179
13.1.3 ENUMERATE THE DEVOPS PROJECT.....	180
<b>CONCLUSION</b> .....	<b>184</b>

**14 LAB - REPOSITORY ACCESS AND PRIVILEGE ESCALATION VIA SERVICE PRINCIPAL ON SELF-HOSTED AGENT ..... 185**

<b>LAB OVERVIEW</b> .....	<b>185</b>
<b>HANDS ON: EXPLOITING MANAGED IDENTITY</b> .....	<b>185</b>
14.1.1 ENUMERATE THE DEVOPS ORGANIZATION.....	185
14.1.2 READING THE FILE CONTENT .....	188
14.1.3 GETTING REVERSE SHELL .....	189
<b>CONCLUSION</b> .....	<b>192</b>

**15 LAB - PIPELINE EXPLOITATION VIA GITHUB TO ACCESS ON-PREM SERVER..... 193**

<b>LAB OVERVIEW</b> .....	<b>193</b>
<b>HANDS ON: EXPLOITING GITHUB</b> .....	<b>193</b>
15.1.1 PERFORMING AGENT .....	193
15.1.2 ENUMERATE AGENT POOL .....	195



15.1.3 CREATING A GITHUB REPO AND GENERATING PAT .....	197
15.1.4 UPDATING THE PIPELINE AND OBTAIN A REVERSE SHELL .....	200
<b>CONCLUSION.....</b>	<b>204</b>

**16 LAB - AKS NODE TAKEOVER VIA AZURE DEVOPS PIPELINES ..... 206**

<b>LAB OVERVIEW .....</b>	<b>206</b>
<b>HANDS ON: ABUSING THE PIPELINE .....</b>	<b>206</b>
16.1.1 LOGIN INTO AZURE PORTAL .....	206
16.1.2 DEVOPS ENUMERATION.....	210
16.1.3 CREATING NEW PIPELINES.....	212
16.1.4 CREATING NEW PIPELINE WITH SELF-HOSTED AGENTS.....	214
16.1.5 CREATING NEW REPO .....	219
16.1.6 RECREATE THE PIPELINE.....	221
16.1.7 PIPELINE JOBS .....	222
16.1.8 STEALING MANAGED IDENTITY ACCESS TOKEN.....	224
16.1.9 USING ACCESS TOKEN WITH AZ POWERSHELL .....	229
16.1.10 STEALING MANAGED IDENTITY TOKEN FOR KUBERNETES.....	231
<b>CONCLUSION.....</b>	<b>234</b>