

Advanced Red Team Operations

Lab Guide





Table of Contents

VERSION CONTROL	10
LICENSING	11
1.1 FORTRA LICENSE DISCLAIMER	11
1.2 MITRE LICENSE	11
2 INTRODUCTION	12
2.1 ABOUT THE ADVANCED RED TEAM OPERATIONS (ARTO) CERTIFICATION COURSE	12
2.2 COURSE APPROACH	12
2.3 COURSE SUPPORT	13
3 LAB ENVIRONMENT	14
3.1 OPERATOR MACHINES	14
3.1.1 SERVER INFORMATION	14
3.1.2 TOPOLOGY	15
3.2 ACTIVE DIRECTORY MACHINES	16
3.2.1 SERVER INFORMATION	16
3.2.2 TOPOLOGY	16
3.3 FINAL LAB OVERVIEW	17
4 LAB 1 – DEPLOYING OUR ENVIRONMENT VIA TERRAFORM.....	20
4.1 LAB OVERVIEW	20
4.1.1 CHECKLIST	20
4.1.2 SYSTEMS CREATED	20
4.2 TERRAFORM SET-UP & INSTALLATION.....	21
4.2.1 COMPILED BINARY	21
4.2.2 MACOS (BREW)	21
4.2.3 WINDOWS (CHOCOLATEY).....	21
4.2.4 UBUNTU/DEBIAN LINUX (APT).....	22
4.3 DEPLOYING THE ENVIRONMENT	26
4.3.1 REQUESTING QUOTA INCREASES FOR VM RESOURCES	18
4.3.2 DEPLOYING THE LAB.....	27
4.3.3 STARTING AND STOPPING INSTANCES	28
4.3.4 DESTROYING THE LAB.....	31
4.4 EXERCISES.....	31
5 LAB 2 – USING GUACAMOLE	32



5.1 LAB OVERVIEW	32
5.1.1 CHECKLIST	32
5.1.2 SYSTEMS USED	32
5.2 ACCESSING YOUR GUACAMOLE INSTANCE	32
5.3 CONSOLE SESSIONS.....	33
5.4 FILE TRANSFER – HOST TO GUACAMOLE ENVIRONMENT	35
5.5 FILE TRANSFER - GUACAMOLE ENVIRONMENT TO HOST	38
5.6 EXERCISES.....	38
<u>6 COMMAND & CONTROL FRAMEWORKS.....</u>	<u>39</u>
6.1 COBALT STRIKE	39
6.2 HAVOC FRAMEWORK.....	39
6.3 MYTHIC FRAMEWORK	39
6.4 SLIVER FRAMEWORK.....	39
6.5 CONCLUSION.....	39
<u>7 LAB 3 – COMMAND & CONTROL – PRIMER.....</u>	<u>41</u>
7.1 LAB OVERVIEW	41
7.1.1 CHECKLIST	41
7.1.2 SYSTEMS USED	41
7.2 COMPONENTS	41
7.3 COBALT STRIKE	42
7.3.1 CLIENT	42
7.3.2 LISTENERS & BEACON TYPES	44
7.3.3 STAGED VS. STAGELESS	56
7.4 HAVOC	58
7.4.1 INSTALLING HAVOC.....	58
7.4.2 CLIENT	61
7.4.3 LISTENERS & BEACON TYPES	64
7.4.4 STAGED VS. STAGELESS	69
7.5 EXERCISES.....	69
<u>8 LAB 4 – COMMAND & CONTROL – DEEP DIVE.....</u>	<u>70</u>
8.1 LAB OVERVIEW	70
8.1.1 CHECKLIST	70
8.1.2 SYSTEMS USED	70
8.2 PROTECTING THE TEAM SERVER.....	70
8.3 STARTING THE TEAM SERVER.....	71
8.3.1 COBALT STRIKE.....	71
8.4 CREATING & USING PROFILES	74
8.4.1 COBALT STRIKE PROFILES	74
8.4.2 HAVOC PROFILES	81
8.5 BEACON OBJECT FILES.....	87
8.5.1 COBALT STRIKE BOFs.....	87



8.5.2 HAVOC BOFs	89
8.6 EXERCISES.....	89
9 LAB 5 – TRAFFIC RELAY & REDIRECTION	90
9.1 LAB OVERVIEW	90
9.1.1 CHECKLIST	90
9.1.2 SYSTEMS USED	90
9.2 INTRODUCTION TO RELAYS & REDIRECTORS	90
9.3 HTTPS REDIRECTOR SETUP	93
9.3.1 HTTP PROXYPASS.....	94
9.4 DOMAIN FRONTING	95
9.4.1 DOMAIN NAMES & DNS CONFIGURATION	95
9.4.2 DOMAIN REGISTRAR BLOCKING	97
9.5 CONFIGURING THE REDIRECTOR	98
9.5.1 TRUSTED TLS CERTIFICATES WITH LET'S ENCRYPT	103
9.5.2 TRUSTED TLS CERTIFICATES WITH CLOUDFLARE	109
9.5.3 TESTING OUR REDIRECTOR.....	110
9.6 EXERCISES.....	115
10 LAB 6 – FORTIFYING OUR REDIRECTOR.....	116
10.1 LAB OVERVIEW	116
10.1.1 CHECKLIST	116
10.1.2 SYSTEMS USED	116
10.2 COMMS FILTERING – USER AGENT.....	117
10.3 COMMS FILTERING – CUSTOM HTTP HEADERS.....	121
10.4 COMMS FILTERING – COBALT STRIKE PROFILE URIs	124
10.5 COMMS FILTERING – IP ADDRESS BLOCKLIST.....	127
10.6 BONUS: CATEGORIZING OUR DOMAIN	131
10.7 LOGGING & DECEPTION.....	131
10.7.1 ADDING LOGGING & A CUSTOM ERROR PAGE TO OUR SERVER	131
10.8 EXERCISES.....	137
11 BONUS LAB – SMB & TCP BEACON DEEP DIVE.....	138
11.1.1 UTILIZING SMB AND TCP BEACONS FOR INTERNAL NETWORK PIVOTING	138
11.1.2 NETWORKING STRATEGIES WITH SMB AND TCP BEACONS.....	138
11.1.3 TCP BEACONS: THE NEW PLAYERS	139
11.1.4 VISUALIZING BEACON CHAINS.....	139
11.1.5 CREATING AN SMB LISTENER FROM THE CS GUI	139
11.1.6 LINKING AND UNLINKING BEACONS IN NETWORK PIVOTING	141
11.1.7 TESTING THE SMB BEACON IN ACTION.....	143
11.1.8 SETTING UP TCP BEACONS FOR ENHANCED NETWORK PIVOTING	146
11.1.9 ENSURING OPERATIONAL SECURITY WITH CUSTOM FRAME HEADERS	148
11.1.10 WHY CUSTOM HEADERS MATTER	148
11.1.11 CUSTOMIZING FOR OPSEC	148



11.2 EXERCISES	149
12 LAB 7 – USING AZURE CDN FOR TRAFFIC REDIRECTION	150
12.1 LAB OVERVIEW	150
12.1.1 CHECKLIST	150
12.1.2 SYSTEMS USED	150
12.2 AZURE SUBSCRIPTION AND RESOURCE PROVIDERS	150
12.3 HTTPS BEACONS OVER AZURE FRONT DOOR	153
12.3.1 CREATING AN AZURE FRONT DOOR INSTANCE	153
12.3.2 CREATING ROUTES IN AZURE FRONT DOOR	156
12.3.3 REVIEW AND CREATE THE AZURE FRONT DOOR PROFILE	159
12.3.4 MODIFYING COBALT STRIKE CACHE HEADERS IN THE PROFILE	160
12.3.5 TESTING THE AZURE FRONT DOOR REDIRECTOR	161
12.3.6 SETTING UP A COBALT STRIKE LISTENER	162
12.3.7 ENSURING FULL COMMUNICATION THROUGH THE REDIRECTOR	164
12.4 HARDENING AZURE FRONT DOOR FOR RED TEAM OPERATIONS	165
12.5 USING CUSTOM DOMAINS WITH AZURE FRONT DOOR	168
12.5.1 PURCHASING A DOMAIN FOR OUR AZURE FRONT DOOR SETUP	169
12.6 EXERCISES	174
13 LAB 8 – USING AZURE APP SERVICES AS REDIRECTORS	175
13.1 LAB OVERVIEW	175
13.1.1 CHECKLIST	175
13.1.2 SYSTEMS USED	175
13.2 SETTING UP THE AZURE WEB APP	175
13.2.1 ACCESSING THE APP SERVICE VIA SSH	178
13.2.2 SETTING UP THE NODE.JS REDIRECTOR	179
13.2.3 CREATING THE FORWARDING APPLICATION	180
13.2.4 CONFIGURING THE STARTUP COMMAND	182
13.2.5 VERIFYING THE REDIRECTOR	183
13.2.6 INTEGRATING WITH COBALT STRIKE	184
13.3 EXERCISES	186
14 LAB 9 – GOOGLE CLOUD PLATFORM REDIRECTION	187
14.1 LAB OVERVIEW	187
14.1.1 CHECKLIST	187
14.1.2 SYSTEMS USED	187
14.2 PREPARING THE GCP ENVIRONMENT	187
14.2.1 DOMAIN PREPARATION WITH CLOUDFLARE	187
14.2.2 SETTING UP A CUSTOM DOMAIN WITH GOOGLE CDN	189
14.3 SETTING UP THE DNS	196
14.4 PREVENTING CACHING	199
14.5 TESTING OUR CUSTOM DOMAIN	199
14.6 USING THE CDN AS A LISTENER	200



15 LAB 10 – CLOUDFRONT REDIRECTION	201
15.1 LAB OVERVIEW	201
15.1.1 CHECKLIST	201
15.1.2 SYSTEMS USED	201
15.2 TRAFFIC REDIRECTION SETUP	201
15.2.1 ORIGIN	203
15.2.2 DEFAULT CACHE BEHAVIOR SETTINGS	205
15.2.3 CACHE KEY SETTINGS	206
15.2.4 WEB APPLICATION FIREWALL (WAF).....	206
15.3 AWS DISTRIBUTION FOR COBALT STRIKE.....	206
15.4 CREATING A MALLEABLE C2 PROFILE FOR AWS	208
15.5 UPDATING APACHE CONFIGURATION FOR CLOUDFRONT TRAFFIC	209
15.6 ADJUSTING COBALT STRIKE LISTENER FOR CLOUDFRONT ROUTING	211
15.7 GENERATING AND VALIDATING COBALT STRIKE BEACON.....	211
15.8 GEO-FILTERING WITH CLOUDFRONT.....	212
15.9 EXERCISES.....	213
16 LAB 11 – SERVERLESS LAMBDA REDIRECTION.....	214
16.1 LAB OVERVIEW	214
16.1.1 USING PYTHON 3.10 FOR AWS LAMBDA.....	214
16.1.2 DEPENDENCY LAYER FOR AWS LAMBDA.....	214
16.1.3 CHECKLIST	215
16.1.4 SYSTEMS USED	215
16.2 LAB PREPARATIONS.....	215
16.3 CONFIGURING THE RELAY.....	217
16.4 TESTING OUR LISTENER	221
16.5 OPSEC CONSIDERATIONS FOR HTTP HEADER-BASED ACCESS CONTROL	222
16.5.1 HOW THIS IS IMPLEMENTED.....	223
16.6 EXERCISES.....	224
17 LAB 12 – USING FLASK & GUNICORN AS A HIGH-SPEED REDIRECTOR.....	225
17.1 LAB OVERVIEW	225
17.1.1 CHECKLIST	225
17.1.2 SYSTEMS USED	225
17.2 DEPLOYING AN AWS UBUNTU SERVER FOR THE FLASK REDIRECTOR	225
17.3 CREATING THE FLASK REDIRECTOR.....	231
17.4 TESTING WITH COBALT STRIKE	233
17.5 AUTOMATING THE DEPLOYMENT WITH FREDI.....	235
17.6 EXERCISES.....	241
18 LAB 13 – MICROSOFT DEV TUNNELS FOR HTTPS C2 TRAFFIC	242
18.1 LAB OVERVIEW	242
18.1.1 CHECKLIST	242



18.1.2 SYSTEMS USED	242
18.2 ACCOUNT SETUP FOR DEV TUNNELS	242
18.3 INSTALLING DEV TUNNELS AND HOSTING A REDIRECTOR	244
18.4 CREATING AND HOSTING THE TUNNEL	247
18.5 BYPASSING MICROSOFT'S ANTI-PHISHING PAGE.....	249
18.6 EXERCISES.....	251
<u>19 IMPORTANT NOTE ON ACTIVE DIRECTORY LAB</u>	<u>252</u>
19.1 OPERATION ERROR EC2: RUNINSTANCES	252
19.2 INSUFFICIENT INSTANCE CAPACITY	252
<u>20 LAB 14 – TOOLING & OFFENSIVE DEVELOPMENT.....</u>	<u>254</u>
20.1 LAB OVERVIEW	254
20.1.1 CHECKLIST	254
20.1.2 SYSTEMS USED	254
20.2 IMPACKET	254
20.2.1 REMCOM.....	254
20.2.2 WMIEXEC.PY	257
20.2.3 SMBEXEC.PY.....	260
20.2.4 SMBSERVER.PY.....	262
20.2.5 DCOMEXEC.PY	266
20.2.6 SECRETS_DUMP.PY	268
20.3 PIVOTING & LATERAL MOVEMENT.....	270
20.3.1 SOCKS	270
20.3.2 PROXYING THROUGH BEACONS.....	272
20.3.3 PROXYCHAINS-NG	272
20.4 NETEXEC	278
20.4.1 BASIC USAGE	278
20.4.2 LOGGING & INTEGRATIONS.....	279
20.4.3 ENUMERATION.....	280
20.4.4 INITIAL ACCESS	281
20.4.5 EXPLOITATION & POST EXPLOITATION TOOLS.....	281
20.4.6 LOOTING SHARES	284
20.5 SHELLCODE LOADERS.....	285
20.5.1 PROCESS INJECTION.....	285
20.5.2 LOLBIN ABUSE	288
20.6 TOOL MODIFICATIONS	291
20.6.1 ETW/AMSI PATCH	291
20.6.2 .NET OBFUSCATION	297
20.6.3 NEO-CONFUSEREX.....	297
20.7 EXERCISES.....	300
<u>21 LAB 15: WINDOW KERNEL INTRODUCTION</u>	<u>301</u>
21.1 BACKGROUND	301



21.2 DEBUGGING THE WINDOWS KERNEL: LOCAL	301
21.3 DEBUGGING THE WINDOWS KERNEL: REMOTE	305
21.4 EXERCISES	305
22 LAB 16: KERNEL TELEMETRY: KERNEL CALLBACK NOTIFICATIONS	305
22.1 PROCESS, THREAD, AND IMAGE LOAD NOTIFICATION CALLBACKS	305
22.2 FINDING NOTIFY ROUTINE ARRAYS	307
22.3 FINDING AN ARRAY ENTRY'S DRIVER FUNCTION	308
22.4 BLINDING THE EDR TO NEW PROCESSES	310
22.5 TELEMETRY REVIEW	315
22.6 EXERCISES	315
23 LAB 17: KERNEL TELEMETRY: EVENT TRACING FOR WINDOWS	316
23.1 BACKGROUND	316
23.2 EVENT TRACING FOR WINDOWS THREAT INTELLIGENCE (ETW-TI) PROVIDER	316
23.3 MONITORING ETW EVENTS	317
23.4 DISABLING ETW IN KERNEL LAND	319
23.5 EXERCISES	323
24 LAB 18: KERNEL PROTECTIONS: PROCESS PROTECTION	324
24.1 BACKGROUND	324
24.2 THE PROTECTION HIERARCHY	325
24.3 FINDING AND MANIPULATING PPL IN EPROCESS	326
24.4 EXERCISES	329
25 LAB 19: ATTACKING THE KERNEL: BRING YOUR OWN VULNERABLE DRIVER (BYOVD)	330
25.1 BACKGROUND	330
25.2 DRIVER SIGNATURE ENFORCEMENT (DSE)	331
25.3 KERNEL VULNERABILITIES	331
25.4 MICROSOFT PROTECTIONS: VULNERABLE DRIVER BLOCK LIST	332
25.5 SUBVERTING OUR LIMITATIONS: WEAPONIZING SIGNED, UNKNOWN VULNERABLE DRIVERS	332
25.6 INSTALLING THE VULNERABLE DRIVER	333
25.7 COMMUNICATING WITH THE DRIVER	333
25.8 ANALYZING THE VULNERABLE DRIVER PoC EXPLOIT	334
25.9 A WORD ON THIS DRIVER	338
25.10 EXERCISES	338
26 LAB 20: BYOVD: DISABLING NOTIFICATION CALLBACKS	339
26.1 BACKGROUND & A WORD ON OFFSETS	339
26.2 CALCULATING OUR OFFSETS	339
26.3 EXPLOITING THE DRIVER TO REMOVE CALLBACKS	340



26.4 EXERCISES.....	342
<u>27 LAB 21: BYOVD: TURNING OFF ETW AND OTHER TELEMETRY.....</u>	<u>343</u>
27.1 READ PRIMITIVE: WALKING THE STRUCTURES	343
27.2 WRITE PRIMITIVE: DISABLING THE ETW-TI PROVIDER.....	344
27.3 EXERCISES.....	346
<u>28 ATTACK PATH CHALLENGE.....</u>	<u>347</u>
28.1 STIGS CORP. COMPANY BACKGROUND	347
28.2 RULES OF ENGAGEMENT	347
28.3 ATTACK METHODOLOGY.....	348
<u>29 INFILTRATING THE STRONGHOLD – ATTACKING STIGS CORP.....</u>	<u>349</u>
29.1 LAB OVERVIEW	349
29.1.1 CHECKLIST	349
29.1.2 SYSTEMS USED	349
29.2 LAB 22 – INITIAL RECONNAISSANCE	350
29.2.1 OPEN-SOURCE INTELLIGENCE.....	350
29.2.2 WEB APPLICATION DISCOVERY	367
29.3 LAB 23 – GAINING ENTRY.....	369
29.3.1 STEPPING THROUGH THE WEB APPLICATION	369
29.3.2 PASSWORD SPRAYING	370
29.4 EXERCISES.....	375
29.5 LAB 24 – INITIAL COMPROMISE.....	376
29.5.1 EXPLORING THE FILE UPLOAD FUNCTIONALITY	376
29.5.2 ESTABLISHING A FOOTHOLD.....	379
29.5.3 GETTING A CALLBACK	381
29.5.4 CONCLUSION.....	387
29.5.5 EXERCISES.....	387
29.6 LAB 25 – LOCAL PRIVILEGE ESCALATION	388
29.6.1 BROWSING THE SYSTEM	389
29.6.2 PIVOTING & LIVING OFF THE FOREIGN LAND	392
29.6.3 PASSWORD SPRAYING THE DOMAIN	393
29.6.4 ELEVATING PRIVILEGES	395
29.6.5 EXERCISES.....	396
29.7 LAB 26 – EXPLOITING MICROSOFT SQL SERVERS THROUGH THICK CLIENTS.....	397
29.7.1 DISCOVERY	397
29.7.2 REVERSING THE APPLICATION.....	402
29.7.3 EXTRACTING CREDENTIALS (STATIC ANALYSIS).....	405
29.7.4 EXTRACTING CREDENTIALS (DYNAMIC ANALYSIS).....	405
29.7.5 ATTACKING THE MSSQL SERVER	407
29.7.6 EXERCISES.....	411
29.8 LAB 27 – LEVERAGING SEIMPERSONATEPRIVILEGE FOR PRIVILEGE ESCALATION.....	412
29.8.1 UNDERSTANDING THE EXPLOIT	412



29.8.2 PRIVILEGE ESCALATION WITH SWEETPOTATO.....	412
29.8.3 EXERCISES.....	414
29.9 LAB 28 – ATTACKING ACTIVE DIRECTORY CERTIFICATE SERVICES (ADCS)	415
29.9.1 ACTIVE DIRECTORY CERTIFICATE SERVICES (ADCS) EXPLAINED.....	415
29.9.2 SETTING UP A SOCKS PROXY WITH CERTIFY FOR AD CS EXPLOITATION	416
29.9.3 HUNTING FOR VULNERABLE ADCS TEMPLATES	417
29.9.4 EXERCISES.....	419
29.10 LAB 29 – DOMAIN DOMINATION – ACHIEVING FULL DOMAIN COMPROMISE	420
29.11 OPERATIONAL MASTERY CHALLENGES.....	420
29.11.1 CHALLENGE 1: COVERT NETWORK MANEUVERING.....	420
29.11.2 CHALLENGE 2: COMMANDING THE COMMAND CENTER.....	420
29.11.3 CHALLENGE 3: EXERTING INFLUENCE WITH DCSYNC	420
29.11.4 CHALLENGE 4: ESCALATING TO SYSTEM	420
29.11.5 CHALLENGE 5: MEMORY MASTERY.....	420
29.11.6 CHALLENGE 6: THE ART OF EXTRACTION OVER SOCKS	420
29.11.7 CHALLENGE 7: HISTORICAL HEIST WITH SECRETS DUMP	420
29.11.8 ESTABLISH A SMB BEACON ON THE ACTIVE DIRECTORY CERTIFICATE SERVICES SERVER.....	421
29.11.9 ESTABLISH A HTTPS BEACON ON THE ACTIVE DIRECTORY DOMAIN CONTROLLER.....	423
29.11.10 EXTRACT CREDENTIAL MATERIAL ABUSING DIRECTORY REPLICATION SERVICE (DRS) REMOTE PROTOCOL (MS-DRSR).....	424
29.11.11 PERFORM PRIVILEGE ESCALATION ON THE ACTIVE DIRECTORY DOMAIN CONTROLLER	427
29.11.12 EXTRACT CREDENTIAL MATERIAL FROM THE LSASS PROCESS IN THE ACTIVE DIRECTORY DOMAIN CONTROLLER	427
29.11.13 EXTRACT CREDENTIAL MATERIAL FROM THE “NTDS.DIT” FILE.....	429
29.11.14 EXTRACT HISTORICAL HASHES USING “SECRETS DUMP.PY” AND DETERMINE ACTIVE/INACTIVE ACCOUNTS	430
<u>30 CAPSTONE CHALLENGE – RAGE AGAINST THE AV/EDR DEFENSES.....</u>	<u>432</u>
30.1 DEPLOY ENVIRONMENT	432
<u>31 APPENDICES</u>	<u>435</u>
31.1 ABBREVIATIONS	435
31.2 ADDITIONAL RESOURCES	435
31.3 CREDENTIALS.....	435