

Offensive Active Directory Operations Certification (OADOC) Lab Guide





Table of Contents

1	<u>LICENSING</u>	<u>20</u>
2	<u>DISTRIBUTION AND CONFIDENTIALITY NOTICE</u>	<u>21</u>
3	<u>INTRODUCTION TO OADOC</u>	<u>22</u>
	ABOUT THE COURSE	22
	AWS REQUIREMENTS	23
	COURSE APPROACH	24
	COURSE SUPPORT	24
4	<u>LAB ENVIRONMENT</u>	<u>25</u>
	TOPOLOGY	25
	EXPLANATION OF THE SERVER INVENTORY TABLE FOR STUDENTS	28
	LAB DEFENSES	31
	LAB ENVIRONMENT ADMINISTRATIVE CREDENTIALS	32
	FINAL LAB OVERVIEW	33
5	<u>DEPLOYING OUR ENVIRONMENT VIA TERRAFORM</u>	<u>34</u>
	LAB OVERVIEW	34
	TERRAFORM SET-UP & INSTALLATION	35
	DEPLOYING THE ENVIRONMENT	38
3.4	EXERCISES	41
6	<u>USING GUACAMOLE</u>	<u>42</u>



LAB OVERVIEW	42
ACCESSING YOUR GUACAMOLE INSTANCE	43
CONSOLE SESSIONS.....	43
FILE TRANSFER - HOST TO GUACAMOLE ENVIRONMENT	46
FILE TRANSFER - GUACAMOLE ENVIRONMENT TO HOST	50
EXERCISES	50
7 TOOLING AND DEVELOPMENT	51
WKL'S APPROACH TO TOOL SELECTION	51
THE TRADE-OFF: TRUST VS. FLEXIBILITY.....	52
LAB TOOLING.....	53
8 ATTACK METHODOLOGY	54
ATTACK METHODOLOGY FOR AD PENTESTING.....	54
APPLYING THESE FRAMEWORKS	58
9 INTRODUCTION TO ACTIVE DIRECTORY.....	59
BASIC OVERVIEW OF ACTIVE DIRECTORY	59
HYBRID INTEGRATION WITH ACTIVE DIRECTORY	60
10 ACTIVE DIRECTORY ENUMERATION AND RECONNAISSANCE.....	65
ENUMERATING THE NETWORK FOR AD INFRASTRUCTURE	65
CORE AD INDICATORS.....	65
HOST CLASSIFICATION RULES	66



KEY COMPONENTS AND TERMINOLOGY.....	66
TARGETED NMAP FOR AD FINGERPRINTING.....	73
<u>11 COMMON ACTIVE DIRECTORY PROTOCOLS.....</u>	<u>74</u>
LAB OVERVIEW	74
LDAP	75
ADWS	78
SERVER MESSAGE BLOCK (SMB).....	82
WINDOWS REMOTE MANAGEMENT (WINRM)	83
WINDOWS MANAGEMENT INSTRUMENTATION (WMI).....	90
INTRODUCTION TO CIM	93
REMOTE PROCEDURE CALL (RPC)	94
MICROSOFT REMOTE PROCEDURE CALL (MS-RPC)	94
DOMAIN NAME SYSTEM (DNS).....	97
LAB OBJECTIVE: BUILDING SIMPLE LDAP CONNECTOR FOR ACTIVE DIRECTORY (PYTHON).....	102
LAB SUMMARY	110
ADDITIONAL EXERCISES	110
<u>12 INTERNAL DNS AND PORT SCANNING.....</u>	<u>111</u>
LAB OVERVIEW	111
INTERNAL DNS	113
WINDOWS BASED ENUMERATION	113
LAB OBJECTIVE USING WINDOWS	118
LINUX-BASED ENUMERATION	121



LAB OBJECTIVE USING LINUX	125
EXERCISES	129
<u>13 PIVOTS & PORT FORWARDING.....</u>	<u>130</u>
LAB OVERVIEW	130
COMMAND & CONTROL METHODOLOGY - THINK BEYOND RDP	130
LAB ENVIRONMENT.....	136
INTRODUCTION TO SOCKS PROXIES	136
PIVOTING FUNDAMENTALS	139
PORT FORWARDING TECHNIQUES.....	140
CHISEL: MODERN TUNNELING TOOL	144
PROXYCHAINS CONFIGURATION	148
PROXIFIER: WINDOWS SYSTEM-LEVEL PROXY ROUTING.....	150
SSH TUNNELLING AND JUMP HOSTS	175
ALTERNATIVE TUNNELLING METHODS	191
COMMON PIVOTING SCENARIOS	217
TROUBLESHOOTING COMMON ISSUES.....	218
PERFORMANCE OPTIMIZATION.....	223
OPERATIONAL SECURITY CONSIDERATIONS	224
SUMMARY	226
<u>14 NULL SESSION & GUEST ACCOUNT EXPLOITATION.....</u>	<u>228</u>
LAB OVERVIEW	228
INTRODUCTION TO NULL SESSIONS & GUEST ACCOUNT	229



MODERN TOOLING - DEPTH & TRIAGE	245
SHARE ANALYSIS, FILE HANDLING AND CREDENTIAL VERIFICATION	251
KEY VULNERABILITIES AND REMEDIATION	254
SUMMARY	255
<u>15 UNDERSTANDING CORE AD COMPONENTS.....</u>	256
DOMAIN CONTROLLERS	256
FORESTS, TREES AND DOMAINS.....	257
USERS, COMPUTERS AND GROUPS.....	259
SERVICE ACCOUNTS.....	260
ORGANIZATIONAL UNITS AND GROUP POLICIES.....	261
KERBEROS	263
TRUSTS	264
<u>16 UNDERSTANDING LDAP, SMB AND OTHER SERVICE BASED ENUMERATION.....</u>	267
WINDOWS BASED ENUMERATION	267
USING AD EXPLORER WITH A SOCKS PROXY	273
USING AD EXPLORER WITH KERBEROS TICKETS.....	274
COMBINING SOCKS PROXYING WITH KERBEROS.....	275
LINUX BASED ENUMERATION	278
UNDERSTANDING SOAP AND ADWS IN ACTIVE DIRECTORY	284
ENUMERATING ADWS USING POWERSHELL	285
ENUMERATING SOAP ENDPOINTS ON THE DOMAIN CONTROLLER	285
HOW SOAP AND ADWS SUPPORT ENUMERATION	286



SAMPLE ENUMERATION FLOW FOR THE OADOC ENVIRONMENT	286
<u>17 ACTIVE DIRECTORY SECURITY TECHNOLOGIES</u>	<u>288</u>
LAPS.....	288
CREDENTIAL GUARD	290
PROTECTED USERS GROUP	292
MANAGED SERVICE ACCOUNTS.....	293
MSA	293
gMSA	294
dMSA	297
<u>18 ENUMERATING ACTIVE DIRECTORY.....</u>	<u>299</u>
LAB OVERVIEW	299
INTRODUCTION	300
WINDOWS AND LINUX ENUMERATION TOOLS.....	300
ENUMERATING THE DOMAIN	301
SUMMARY	381
<u>19 AUTOMATING AD ENUMERATION</u>	<u>382</u>
LAB OVERVIEW	382
INTRODUCTION	383
BLOODHOUND	383
INSTALLING AND CONFIGURING BLOODHOUND (COMMUNITY EDITION).....	384
PINGCASTLE.....	394



AD MINER	395
NESSUS	396
LAB OBJECTIVE USING WINDOWS.....	397
USING ACTIVE DIRECTORY EXPLORER WITH KERBEROS TICKETS.....	408
LAB OBJECTIVE USING LINUX.....	409
OPSEC BEST PRACTICES	413
LAB SUMMARY	414
<u>20 PASSWORD ATTACKS IN ACTIVE DIRECTORY</u>	<u>415</u>
<u>21 INTERNAL PASSWORD SPRAYING.....</u>	<u>417</u>
LAB OVERVIEW	417
INTRODUCTION TO PASSWORD SPRAYING	418
WINDOWS-BASED SPRAYING.....	422
LAB OBJECTIVE USING WINDOWS.....	426
LINUX BASED SPRAYING.....	429
PASSWORD SPRAYING.....	431
LAB OBJECTIVE USING LINUX	433
LAB SUMMARY	435
ADDITIONAL EXERCISES	436
<u>22 LOGGING AND AMSI BASED BYPASSES.....</u>	<u>437</u>
LAB OVERVIEW	437
POWERSHELL LOGGING BYPASSES.....	438
POWERSHELL LOGGING MECHANISMS	438



KEY COMPONENTS AND TERMINOLOGY.....	439
POWERSHELL LOGGING EVASION TECHNIQUES	441
BYPASSING AMSI	455
LAB OBJECTIVE USING CUSTOM OBFUSCATION OR ADVANCED HARDWARE BREAKPOINTS.....	466
LAB SUMMARY	478
ADDITIONAL EXERCISES	479
<u>24 LDAP OBFUSCATION.....</u>	480
LAB OVERVIEW	480
INTRODUCTION	481
LDAP SEARCH FILTER OBFUSCATION.....	481
WINDOWS BASED OBFUSCATION	485
LAB OBJECTIVE USING WINDOWS	494
LINUX BASED OBFUSCATION.....	498
<u>25 KERBEROS</u>	499
LAB OVERVIEW	499
INTRODUCTION TO KERBEROS	500
KERBEROS AUTHENTICATION	501
KERBEROS BASICS IN ACTIVE DIRECTORY	501
CORE BUILDING BLOCKS	504
WORKING WITH RUBEUS	507
PKINIT, SHADOW CREDENTIALS, AND UNPAC-THE-HASH.....	512
KERBEROS RELAY	515



26 ACL ATTACKS IN AD	518
LAB OVERVIEW	518
INTRODUCTION TO ACL ATTACKS	519
SDDL (SECURITY DESCRIPTOR DEFINITION LANGUAGE)	519
ACL VERIFICATION IN WINDOWS.....	520
INTRODUCTION TO DACLS.....	521
INTRODUCTION TO SACLs.....	524
WINDOWS BASED DACL ENUMERATION	525
LINUX BASED DACL ENUMERATION.....	530
ATTACK OBJECTIVE	535
WINDOWS BASED DACL ABUSE.....	536
LINUX BASED DACL ABUSE.....	545
LAB SUMMARY	554
27 KERBEROASTING AND ASREPROASTING	555
LAB OVERVIEW	555
INTRODUCTION TO SERVICE ACCOUNTS	556
INTRODUCTION TO ASREPROASTING.....	557
INTRODUCTION TO KERBEROASTING	561
INTRODUCTION TO ASREQROASTING	566
WINDOWS BASED EXPLOITATION	568
LINUX BASED EXPLOITATION.....	580
BLIND KERBEROASTING.....	590
LAB SUMMARY	596



<u>28 RDP PASSWORD SPRAYING</u>	597
LAB OVERVIEW	597
EXPANDING ACCESS THROUGH CREDENTIAL REUSE	597
ENUMERATING RDP ENABLED SYSTEMS	598
TEST RDP AUTHENTICATION	599
LAB SUMMARY	603
<u>29 DELEGATION ATTACKS IN AD</u>	605
INTRODUCTION TO DELEGATION ATTACKS	605
<u>30 SPN JACKING</u>	612
LAB OVERVIEW	612
HOW SPN JACKING WORKS	613
LINUX EXPLOITATION	614
WINDOWS EXPLOITATION	623
LAB SUMMARY	631
<u>31 POTATO EXPLOITS - IMPROPER SERVICE PERMISSIONS & TOKEN DUPLICATION ABUSE</u> ..	634
LAB OVERVIEW	634
EVALUATING SERVICE CONTROL MANAGER PERMISSIONS	635
IDENTIFY WRITABLE DIRECTORIES	636
LOCATE VULNERABLE SERVICE BINARY	637
CONFIRM SERVICE PERMISSIONS	637
MATRIXAGENT REVERSE SHELL CODE	640



BACKUP AND REPLACE THE SERVICE BINARY	643
SERVICE BINARY REPLACEMENT	644
PRIVILEGE ESCALATION VIA GODPOTATO	647
ESTABLISH PERSISTENCE AS SYSTEM	651
VERIFY PERSISTENCE	652
UNDERLYING VULNERABILITIES	652
SUMMARY	654
<u>32 DUMPING CREDENTIALS</u>	<u>655</u>
LAB OVERVIEW	655
UAC REMOTE RESTRICTIONS & LOCAL ACCOUNT TOKEN FILTER POLICY	678
SUMMARY	682
<u>33 INTRODUCTION TO MSSQL</u>	<u>683</u>
HIGH-LEVEL ENUMERATION METHODOLOGY	684
DEFAULT/SYSTEM DATABASES	685
COMMON SERVER-SIDE OBJECTS AND PROCEDURES	686
SQL SERVER – ROLES AND PRIVILEGES	687
<u>34 FROM ENUMERATION TO EXECUTION: TARGETING MICROSOFT SQL SERVER</u>	<u>691</u>
ENUMERATING MSSQL	692
AUTHENTICATED MSSQL ACCESS TESTING	696
ACCESSING THE BACKUP SHARE AND EXTRACTING CREDENTIALS	701
ENUMERATION & POST-EXPLOITATION	705



SQL AGENT POWERSHELL ATTACK PATH	710
SUMMARY	726
<u>35 SQL IMPERSONATION TO RCE VIA XP_CMDSHELL.....</u>	<u>728</u>
BACKGROUND: WHAT IMPERSONATION IS AND WHY IT MATTERS.....	728
WHAT XP_CMDSHELL IS AND WHY WE TARGET IT	730
COMMANDS READY TO RUN FROM SQLCMD.....	731
RUNNING THE REVERSE-SHELL PAYLOAD VIA XP_CMDSHELL	733
SHARPEFSPOTATO - MS-EFSR LOCAL PRIVILEGE ESCALATION	737
<u>36 PRIVILEGE ESCALATION VIA LINKED SQL SERVERS AND MISCONFIGURED STORED PROCEDURE</u>	<u>754</u>
LAB INFORMATION.....	754
CHECKLIST	754
SYSTEMS USED.....	754
LAB OVERVIEW	755
IMPORTANT FORK IN THE PATH (STUDENT CHOICE)	756
LAB ENVIRONMENT.....	757
ATTACK PATH OVERVIEW	758
LAB WALKTHROUGH	760
LAB COMPLETE.....	769
SUMMARY	769
<u>37 ACHIEVING REMOTE CODE EXECUTION ON MSSQL02 USING UNSAFE CLR</u>	<u>771</u>



LAB INFORMATION	771
CHECKLIST	771
SYSTEMS USED	771
LAB OVERVIEW	772
LAB ENVIRONMENT CONTEXT	773
ATTACK PATH OVERVIEW	773
UNDERSTANDING CLR ASSEMBLIES AND CODE EXECUTION	775
THE MALICIOUS CLR ASSEMBLY	776
LAB WALKTHROUGH	778
ADVANCED EXPLOITATION: LAUNCHING A REVERSE SHELL	786
LAB COMPLETE	787
SUMMARY	788
<u>38 KERBEROS TICKET EXTRACTION AND DOMAIN COMPROMISE (MATRIX)</u>	<u>790</u>
LAB OVERVIEW	790
SUMMARY	812
<u>39 SQL SERVER CREDENTIAL HARVESTING - EXTRACTING AND CRACKING WINDOWS DOMAIN CREDENTIALS</u>	<u>815</u>
SYSTEMS USED	815
LAB WALKTHROUGH	816
LAB SUMMARY	832
<u>40 SHADOW CREDENTIALS</u>	<u>833</u>



LAB OVERVIEW	833
SHADOW CREDENTIALS ABUSE.....	834
SUMMARY	841
<u>41 WINDOWS LOCAL ADMINISTRATOR PASSWORD SOLUTION (LAPS) EXPLOITATION.....</u>	<u>843</u>
INTRODUCTION TO LAPS	844
THE EVOLUTION OF LAPS	846
LAB ENVIRONMENT CONFIGURATION	851
ABUSING LEGACY LAPS (v1) - THEORY ONLY	867
ABUSING WINDOWS LAPS (v2) - LAB FOCUS.....	869
LAB WALKTHROUGH - WINDOWS-BASED EXPLOITATION	872
LAB WALKTHROUGH - LINUX-BASED EXPLOITATION.....	904
LAB SUMMARY	920
EXERCISES	926
<u>42 ACCOUNT OPERATORS PRIVILEGE ESCALATION - ACL ABUSE AND ADMINSDHOLDER BYPASS</u>	<u>927</u>
INTRODUCTION TO ACCOUNT OPERATORS	929
LAB WALKTHROUGH - PART 1: ADMINSDHOLDER BYPASS	935
LAB WALKTHROUGH - PART 2: BLOODHOUND ACL ANALYSIS.....	949
LAB WALKTHROUGH - PART 3: ADCS ATTACK PREREQUISITES	955
LAB WALKTHROUGH - PART 4: IT SECURITY INFRASTRUCTURE ACCESS	962
LAB SUMMARY	978
EXERCISES	981



<u>44 GROUP MANAGED SERVICE ACCOUNT (GMSA) PASSWORD RETRIEVAL</u>	982
LAB CHECKLIST	983
SYSTEMS USED	983
PREREQUISITES.....	984
INTRODUCTION TO GROUP MANAGED SERVICE ACCOUNTS	984
LAB WALKTHROUGH	991
EXERCISES	1020
<u>45 INTRODUCTION TO DMSA.....</u>	1021
<u>46 KERBEROS TICKET FORGERY AND DOMAIN PERSISTENCE.....</u>	1022
LAB OVERVIEW	1022
FORGED KERBEROS TICKETS OVERVIEW	1022
FORGING KERBEROS TICKETS.....	1024
<u>47 CHILD TO PARENT ESCALATION.....</u>	1045
LAB OVERVIEW	1045
UNDERSTANDING CHILD-TO-PARENT DOMAIN ESCALATION	1046
ATTACKING CHILD-TO-PARENT TRUSTS.....	1046
<u>48 CROSS FOREST ATTACKS</u>	1058
LAB OVERVIEW	1058
SID FILTERING	1058
ENUMERATE FOREST TRUST FROM WINDOWS	1058



ENUMERATING FOREST TRUSTS FROM LINUX	1059
GOLDEN TICKET ATTACK	1059
SIDHISTORY ABUSE.....	1060
TRUST ACCOUNT ATTACK.....	1060
CROSS-FOREST KERBEROASTING	1061
<u>49 ACTIVE DIRECTORY CERTIFICATE SERVICES (AD CS) EXPLOITATION</u>	<u>1062</u>
LAB OVERVIEW	1062
AD CS OVERVIEW	1062
ATTACKING AD CS	1064
LAB ATTACK PATH.....	1091
<u>50 ABUSING SCCM IN ACTIVE DIRECTORY ENVIRONMENTS.....</u>	<u>1113</u>
LAB OVERVIEW	1113
SCCM OVERVIEW	1113
SCCM ATTACK TECHNIQUES OVERVIEW	1116
PREREQUISITES AND TOOL SETUP.....	1117
RECONNAISSANCE (RECON)	1118
SYSTEM MANAGEMENT CONTAINER.....	1119
MSSMSSITE (SITES).....	1119
MSSMSMANAGEMENTPOINT (MPs).....	1119
PREDICTABLE NAMING.....	1119
EXAMPLES	1120
IMPACT	1123



DEFENSIVE IDS	1123
LAB ATTACK PATH.....	1173
<u>51 VIRTUAL SMART CARDS.....</u>	<u>1189</u>
<u>52 DOMAIN DOMINANCE AND PERSISTENCE.....</u>	<u>1190</u>
<u>53 APPENDICES</u>	<u>1191</u>
<u>54 ABBREVIATIONS.....</u>	<u>1191</u>
<u>55 ADDITIONAL RESOURCES.....</u>	<u>1192</u>
<u>56 RECOMMENDED READING</u>	<u>1194</u>
<u>57 TOOLS AND FRAMEWORKS FOR FURTHER EXPLORATION</u>	<u>1195</u>
<u>58 SUGGESTED STUDENT CHALLENGES</u>	<u>1196</u>
<u>59 COURSE ACKNOWLEDGMENT.....</u>	<u>1196</u>