BTFM

Blue Team Field Manual

Version 1.2

Alan White & Ben Clark

BTFM

Blue Team Field Manual

BIBLIOTEKA
Nr ewid. ....
Akademii Sztuki Wojennej

Alan White
Ben Clark

Version 1, Rel 2

BTFM. Copyright © 2017 by Alan White and Ben Clark

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, without prior written permission of the copyright owner.

ISBN-13: 978-1541016361
ISBN-10: 154101636X

Technical Editor: Matt Hulse

Product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, the author uses the names only in an editorial fashion, with no intention of infringement of the trademark. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

The information in this book is distributed "as is". While every precaution was taken to ensure the accuracy of the material, the author assumes no responsibility or liability for errors or omissions, or for damages resulting from the use of the information contained herein.

PREFACE

BTFM Command-Line Syntax:

Notation	Description
#	Generic Linux/*nux shell prompt, sudo may also be used with $
C:\>	Windows Prompt, may require Administrator CMD prompt
PS C:\>	Windows PowerShell
>	Generic prompt, multi OS
<IP ADDRESS>, <PORT>, <USER>, <PASSWORD>, etc.	Requires user determined input and remove <> brackets
-	Caution use of copy/paste with dash/hyphens. en/em/dash ,–,— hyphen -
spaces	Ensure you check spaces and no spaces in commands.

Updates, Edits and Supplement Material:

Ref. http://www.blueteamfieldmanual.com

BTFM is based on the NIST Cybersecurity Framework:

Ref. http://www.nist.gov/cyberframework/

TABLE OF CONTENTS

TABLE OF CONTENTS 4

0 PREPARATION (DOCUMENTATION REVIEW) 8

KEY DOCUMENTS 9
REVIEW 9

1 IDENTIFY (SCOPE) 10

SCANNING AND VULNERABILITIES 11
NMAP 11
NESSUS 11
OPENVAS 12
WINDOWS 13
NETWORK DISCOVERY 13
DHCP 13
DNS 13
HASHING 14
NETBIOS 15
USER ACTIVITY 15
PASSWORDS 15
MICROSOFT BASELINE SECURITY ANALYZER (MBSA) 16
ACTIVE DIRECTORY INVENTORY 16
LINUX 19
NETWORK DISCOVERY 19
DHCP 19
DNS 19
HASHING 20
NETBIOS 20
PASSWORDS 20

2 PROTECT (DEFEND) 21

WINDOWS 22
DISABLE/STOP SERVICES 22
HOST SYSTEM FIREWALLS 22
PASSWORDS 24
HOST FILE 24
WHITELIST 25
APPLICATION RESTRICTIONS 25
IPSEC 28
ACTIVE DIRECTORY (AD) - GROUP POLICY OBJECT (GPO) 30
STAND ALONE SYSTEM - WITHOUT ACTIVE DIRECTORY (AD) 30
LINUX 34
DISABLE/STOP SERVICES 34
HOST SYSTEM FIREWALLS 35
PASSWORDS 36
HOST FILE 37
WHITELIST 37
IPSEC 38

3 DETECT (VISIBILITY) 40

NETWORK MONITORING 41
TCPDUMP 41
TSHARK 43
SNORT 45
NETWORK CAPTURE (PCAP) TOOLS 47
EDITCAP 47
MERGECAP 47
HONEY TECHNIQUES 48
WINDOWS 48
LINUX 49
NETCAT 50
PASSIVE DNS MONITORING 50
LOG AUDITING 51
WINDOWS 51
LINUX 57

4 RESPOND (ANALYSIS) 59

LIVE TRIAGE - WINDOWS 60
SYSTEM INFORMATION 60
USER INFORMATION 60
NETWORK INFORMATION 61
SERVICE INFORMATION 61
POLICY, PATCH AND SETTINGS INFORMATION 62
AUTORUN AND AUTOLOAD INFORMATION 62
LOGS 67
FILES, DRIVES AND SHARES INFORMATION 68
LIVE TRIAGE - LINUX 71
SYSTEM INFORMATION 71
USER INFORMATION 71
NETWORK INFORMATION 72
SERVICE INFORMATION 72
POLICY, PATCH AND SETTINGS INFORMATION 73
AUTORUN AND AUTOLOAD INFORMATION: 73
LOGS 74
FILES, DRIVES AND SHARES INFORMATION 74
MALWARE ANALYSIS 77
STATIC ANALYSIS BASICS 77
IDENTIFY MALWARE 80
PROCESS EXPLORER 80
FILE HASH ANALYSIS 82
HASH QUERY 82
HARD DRIVE AND MEMORY ACQUISITION 83
WINDOWS 83
LINUX 84

5 RECOVER (REMEDIATE) 86

PATCHING 87
WINDOWS 87
LINUX 87
BACKUP 89
WINDOWS 89
LINUX 92

KILL MALWARE PROCESS 93
WINDOWS 93
LINUX 93

6 TACTICS (TIPS & TRICKS) 94

OS CHEATS 95
WINDOWS 95
LINUX 97
DECODING 99
HEX CONVERSION 99
SNORT 101
SNORT RULES 101
DOS/DDOS 104
FINGERPRINT DOS/DDOS 104
TOOL SUITES 106
PREBUILT ISO, VIRTUAL MACHINE AND DISTRIBUTIONS 106

7 INCIDENT MANAGEMENT (CHECKLIST) 108

INCIDENT RESPONSE CHECKLIST 109
IDENTIFICATION TASKS 109
CONTAINMENT TASKS 111
REMEDIATION TASKS 112
OTHER / LESSONS LEARNED TASKS 114
MALWARE ATTRIBUTES CHECKLIST 115

8 SECURITY INCIDENT IDENTIFICATION (SCHEMA) 118

VOCABULARY FOR EVENTS RECORDING AND INCIDENT SHARING (VERIS) 119
GENERAL 119
ACTOR 121
ACTION 122
ASSET 125
ATTRIBUTE 126
COURSE OF ACTION 127
KILL CHAIN MAPPING 128
GATHER DATA FOR MAPPING KILL CHAIN 128
PRIORITIZED DEFENDED ASSET LIST (PDAL) 129
GATHER DATA AND PRIORITIZE ASSETS TO DEFEND 129

10 INDEX (A-Z) 132

Biblioteka Główna
Akademii Sztuki Wojennej
26618/III (CB)
03-026618-000-0

ISBN 9781541016361
90000
9 781541 016361