

# Obsah

PODĚKOVÁNÍ	XV
PŘEDMLUVA	XVI
ÚVOD	XVIII

## Část 1

<b>POZNÁVÁNÍ SOUVISLOSTÍ: ZÁKLADY REAKCE NA INCIDENT</b>	<b>1</b>
--	----------

### *Kapitola 1*

<b>TI VENKU A TI UVNITŘ: PŘÍPADOVÁ STUDIE</b>	<b>3</b>
---	----------

ZNESNADNĚNÍ ÚTOČNÍKOVY SITUACE	4
VNITŘNÍ NEPŘÍTEL	5
INFORMACE ZÍSKANÉ POMOCÍ SOUDNÍHO PŘÍKAZU 18 U.S.C. § 2703	11
TAKŽE?	12

### *Kapitola 2*

<b>ÚVOD DO REAKCÍ NA INCIDENTY</b>	<b>13</b>
------------------------------------	-----------

CÍLE	14
METODOLOGIE REAKCE NA INCIDENT	14
PŘÍPRAVA NA INCIDENT	16
DETEKOVÁNÍ INCIDENTŮ	16
POČÁTEČNÍ REAKCE	17
FORMULACE STRATEGIE REAKCE NA INCIDENT	18
Důležitá rozhodnutí	19
Prezentace možných postupů managementu	20
FORENZNÍ DUPLIKACE KRITICKÝCH DAT	21
VYŠETŘOVÁNÍ	21
IMPLEMENTACE BEZPEČNOSTNÍCH OPATŘENÍ	22
MONITOROVÁNÍ SÍTĚ	23
Rozhodnutí KDE a JAK monitorovat	24
Rozhodnutí CO monitorovat	24

<b>OBNOVA</b>	<b>25</b>
Identifikace rozsahu poškození	25
Výběr strategie obnovy	26
<b>DOKUMENTACE</b>	<b>26</b>
<b>TAKŽE?</b>	<b>27</b>

## **Kapitola 3**

### **PŘÍPRAVA REAKCE NA INCIDENT** **29**

---

#### **IDENTIFIKACE VAŠICH VITÁLNÍCH AKTIV** **30**

#### **PŘÍPRAVA JEDNOTLIVÝCH POČÍTAČŮ** **31**

Zaznamenávání kryptografických kontrolních součtů důležitých souborů 32

Spuštění nebo rozšíření auditu systému 34

Logy aplikací 30

Zabezpečení serveru 39

Záloha důležitých dat 40

Vzdělávání uživatelů v problematice bezpečnosti počítače 41

#### **PŘÍPRAVA SÍTĚ** **42**

Instalace firewallů a IDS 42

Použití filtrů 43

Návrh síťové topologie usnadňující monitorování 43

Šifrování síťového provozu 44

Vyžadování autentizace 45

#### **IMPLEMENTACE ODPOVÍDAJÍCÍ BEZPEČNOSTNÍ POLITIKY A PROCEDUR** **45**

Definování vašeho postoje k incidentu 45

Vypracování politiky přípustného využití 51

Postup návrhu uživatelské politiky 53

Procedury reakce na incidenty 54

#### **TVORBA TOOLKITU REAKCE NA INCIDENTY** **54**

Hardware 55

Software 55

Nástroje určené k monitorování sítí 56

#### **USTANOVENÍ TÝMU REAKCE NA INCIDENTY** **56**

Definice cílů 57

Sestavení týmu 57

Školení poskytovaná specialisty na incidenty 58

#### **TAKŽE?** **59**

## Část 2

## NASAZOVÁNÍ RUKAVIC: SEZNÁMENÍ S TECHNICKÝMI DETAILY

61

## Kapitola 4

## PÁTRACÍ POSTUPY

63

## POČÁTEČNÍ VYŠETŘOVÁNÍ

64

Kladení dotazů o incidentu

65

## POČÁTEČNÍ INFORMACE O INCIDENTU

65

Analýza topologie sítě

66

Ověření platných politik

67

## VYŠETŘOVÁNÍ INCIDENTU

67

Vedení výslechů

68

Počáteční analýza systému

69

## FORMULACE STRATEGIE REAKCE NA INCIDENT

70

Určení vhodného typu reakce

70

Rozpoznání typu útoku

71

Klasifikace napadeného systému

72

Zhodnocení dalších vlivů

72

Podpora managementu

72

## TAKŽE?

73

## Kapitola 5

## POČÍTAČOVÉ VYŠETŘOVÁNÍ

75

## JAK NAKLÁDAT S DŮKAZY

76

Běžné chyby při manipulaci s důkazy

77

Pravidla pro manipulaci s důkazy (Best Evidence Rules)

77

Opatření k zabezpečení úschovy důkazů

78

## POČÁTEČNÍ REAKCE

81

Dočasná data

81

Analýza živého systému

82

## FORENZNÍ DUPLIKOVÁNÍ SYSTÉMU

83

Různé přístupy k procesu duplikace

84

Prověření konfigurace systému

84

Duplikační nástroje

87

## SAFEBACK

88

Vytvoření bootovací diskety

88

Vytvoření duplikátu pomocí programu Safeback

90

## DUPLIKACE POMOCÍ UTILIT OPERAČNÍHO SYSTÉMU UNIX

95

Vytvoření bootovacího disku	96
Vytvoření obrazu disku pomocí dd	96
<b>POUŽITÍ PROGRAMU ENCASE</b>	<b>97</b>
Vytváření důkazních souborů	99
Prohlížení důkazního média	100
<b>VYHLEDÁVÁNÍ DŮKAZŮ</b>	<b>101</b>
Fyzická analýza	102
Logická analýza	103
Kde se důkazy nacházejí	104
<b>TAKŽE?</b>	<b>110</b>

## Kapitola 6

### SÍŤOVÉ PROTOKOLY A TRASOVÁNÍ DAT 111

<b>PROTOKOLY TCP/IP A JEJICH PRINCIPY</b>	<b>112</b>
<b>ENKAPSULACE</b>	<b>113</b>
Hlavička IP-datagramu	115
Hlavička TCP segmentu	119
Hlavička UDP-paketu	122
<b>SNIFFERY</b>	<b>124</b>
<b>TRASOVÁNÍ</b>	<b>125</b>
Ukládání zachycených dat do souborů	127
<b>TAKŽE?</b>	<b>129</b>

## Kapitola 7

### PROVÁDĚNÍ SÍŤOVÉHO DOZORU 131

<b>PROČ PROVÁDĚT SÍŤOVÝ DOZOR?</b>	<b>132</b>
<b>SÍŤOVÉ DŮKAZY</b>	<b>133</b>
Opatření k zabezpečení úschovy důkazů	134
<b>SÍŤOVÉ SOUDNICTVÍ</b>	<b>135</b>
Výzvy síťového soudnictví	135
<b>PŘÍPRAVA VAŠEHO SYSTÉMU</b>	<b>137</b>
Zvolte vhodný software	139
Umístění a bezpečnost monitorovacího softwaru	142
<b>PROVÁDĚNÍ DOZORU</b>	<b>143</b>
Monitorování protokolu telnet	143
Monitorování protokolu FTP	152
Monitorování webového provozu	160
<b>INTERPRETACE SÍŤOVÉHO ÚTOKU</b>	<b>162</b>
<b>TAKŽE?</b>	<b>166</b>

## Kapitola 8

### POKROČILÝ SÍŤOVÝ DOZOR

167

#### HLAVNÍ CÍLE ÚTOČNÍKŮ

168

Činnosti, které obvykle nejsou monitorovány 168

Činnosti, které lze jen těžko odhalit 169

Činnosti, které lze jen těžko zpětně přehrát 170

Činnosti, které je obtížné vysledovat až ke zdrojové adrese IP 171

Co největší zkomplikování sběru důkazů 171

Zachování hodnověrné popiratelnosti 172

#### NASTAVOVÁNÍ SKRYTÝCH KANÁLŮ ICMP

172

Rozeznání skrytých kanálů Loki 176

Rozeznání nové generace skrytých kanálů protokolu ICMP 190

#### NASTAVOVÁNÍ SKRYTÝCH KANÁLŮ PROSTŘEDNICTVÍM BEZSTAVOVÉHO PROTOKOLU TCP

182

Zkoumání bezstavového protokolu TCP 182

Rozpoznání nastavení skrytých kanálů prostřednictvím bezstavového protokolu TCP 183

#### NASTAVOVÁNÍ KANÁLŮ PROTOKOLU HTTP

184

#### ODHALENÍ ILEGÁLNÍCH SERVERŮ

188

#### TAKŽE?

189

## Část 3

### VYŠETŘOVÁNÍ: OPERAČNÍ SYSTÉMY

191

## Kapitola 9

### POČÁTEČNÍ REAKCE NA WINDOWS NT/2000

193

#### VYTVOŘENÍ SADY ZÁCHRANNÝCH NÁSTROJŮ

194

Popisky sady nástrojů 194

Obsah sady nástrojů 195

#### UKLÁDÁNÍ INFORMACÍ ZÍSKANÝCH BĚHEM POČÁTEČNÍ ODEZVY

197

#### ZÍSKÁNÍ NESTÁLÝCH DAT PŘED FOREZNÍ DUPLIKACÍ

199

Organizování a dokumentování vyšetřování 200

Spuštění důvěryhodného příkazového řádku cmd.exe 201

Určování uživatelů přihlášených do systému 202

Určení otevřených portů a naslouchajících aplikací 203

Výpis všech spuštěných procesů 205

Výpis aktuálních a nedávných spojení 207

Dokumentace příkazů použitých během počáteční reakce 207

Vytvoření dávky pro počáteční reakci 208

#### PROVÁDĚNÍ HLOUBKOVÉ, AKTIVNÍ REAKCE

209

Získávání protokolů událostí během aktivní reakce 209

Prozkoumávání registru během aktivní odezvy 213

Získání údajů o času poslední modifikace, vytvoření a přístupu ke všem souborům	215
Získávání systémových hesel	215
Výpis systémové paměti RAM	216
<b>JE FORENZNÍ DUPLIKACE NUTNÁ? TAKŽE?</b>	<b>216</b>

## Kapitola 10

### VYŠETŘOVÁNÍ OPERAČNÍHO SYSTÉMU WINDOWS NT/2000 217

<b>KDE SE V OPERAČNÍM SYSTÉMU WINDOWS NT/2000 NACHÁZÍ DŮKAZY</b>	<b>218</b>
<b>ZŘÍZENÍ FORENZNÍ PRACOVNÍ STANICE</b>	<b>219</b>
Přezkoumávání logických souborů	219
Manipulace s hesly	220
Provádění počáteční analýzy nižší úrovně	222
<b>VYŠETŘOVÁNÍ SYSTÉMU WINDOWS NT/2000</b>	<b>222</b>
Průzkum všech příslušných souborů logů	223
Vyhledávání klíčových slov	229
Prozkoumávání důležitých souborů	230
Identifikace neoprávněných uživatelských účtů nebo skupin	246
Identifikace podvodných procesů	247
Hledání neobvyklých nebo skrytých souborů	247
Kontrola neoprávněných přístupových bodů	249
Průzkum úkolů spuštěných pomocí služby Scheduler Service	252
Analýza vztahů důvěry	253
Průzkum bezpečnostních identifikátorů (SID)	253
<b>AUDIT SOUBORŮ A KRÁDEŽ INFORMACÍ</b>	<b>254</b>
<b>CO UDĚLAT PO ODCHODU ZAMĚSTNANCE</b>	<b>257</b>
Průzkum vyhledávání a použitých souborů	257
Řízení vyhledávání řetězců na pevném disku	258
<b>TAKŽE?</b>	<b>258</b>

## Kapitola 11

### POČÁTEČNÍ REAKCE V UNIXOVÝCH SYSTÉMECH 259

<b>VYTVORENÍ SADY NÁSTROJŮ PRO REAKCI</b>	<b>260</b>
<b>UKLÁDÁNÍ INFORMACÍ ZÍSKANÝCH BĚHEM POČÁTEČNÍ REAKCE</b>	<b>261</b>
<b>ZÍSKÁNÍ NESTÁLÝCH DAT PŘED FORENZNÍ DUPLIKACÍ</b>	<b>262</b>
Spouštění důvěryhodného příkazového řádku	263
Kdo je v systému přihlášen	264
Odhalení sad administrátorských nástrojů LKM	266
Zjišťování otevřených portů a aplikací, které odposlouchávají	267
Průzkum systému souborů /proc	272
Zametání stop	276

<b>PROVEDENÍ KVALITNÍ AKTIVNÍ REAKCE</b>	<b>276</b>
Zjištění doby úprav, přístupu a vytvoření všech souborů	276
Získávání systémových logů během aktivní reakce	277
Získávání důležitých konfiguračních souborů	278
Výpis systémové paměti RAM	279
<b>TAKŽE?</b>	<b>279</b>

## Kapitola 12

### **VYŠETŘOVÁNÍ UNIXU** **281**

<b>PŘÍPRAVA K PRŮZKUMU RESTAUROVANÉHO OBRAZU</b>	<b>282</b>
Zavádění nativního operačního systému	282
Provádění počáteční analýzy nižší úrovně	283
<b>ŘÍZENÍ VYŠETŘOVÁNÍ SYSTÉMU UNIX</b>	<b>283</b>
Průzkum důležitých souborů logů	284
Vyhledávání klíčových slov	289
Průzkum důležitých souborů	291
Identifikace neoprávněných uživatelských účtů a skupin	297
Kontrola neoprávněných přístupových bodů	299
Analýzy vztahů důvěry	299
<b>TAKŽE?</b>	<b>300</b>

## Část 4

### **ANALÝZA PLATFORMOVĚ NEZÁVISLÝCH TECHNOLOGIÍ** **301**

## Kapitola 13

### **VYŠETŘOVÁNÍ SMĚROVAČŮ** **303**

<b>ZÍSKÁVÁNÍ NESTÁLÝCH DAT PŘED VYPNUTÍM</b>	<b>304</b>
Vytvoření spojení se směrovačem	304
Zaznamenávání systémového času	305
Zjišťování přihlášených uživatelů	305
Zjištění provozní doby směrovače	306
Určování naslouchajících socketů	306
Ukládání konfigurace směrovače	307
Prozkoumávání směrovací tabulky	308
Kontrola konfigurací rozhraní	309
Prohlížení vyrovnávací paměti ARP	309
<b>HLEDÁNÍ DŮKAZŮ</b>	<b>310</b>
Postup při přímém ohrožení	310
Postup při krádeži informací	312

<b>SMĚROVAČE JAKO NÁSTROJE PRO REAKCI</b>	<b>214</b>
Seznámení s ACL (Access Control List)	314
Monitorování pomocí směrovačů	317
Reakce na útoky DDoS	317
<b>TAKŽE?</b>	<b>318</b>

## **Kapitola 14**

### **VYŠETŘOVÁNÍ WEBOVÝCH ÚTOKŮ** **319**

<b>DŘÍVE, NEŽ TO SPUSTÍTE</b>	<b>320</b>
<b>HLEDÁNÍ DŮKAZU</b>	<b>320</b>
Zkoumání souborů logů	321
Vyšetřování zohavení webových stránek	326
Vyšetřování útoků na aplikační úrovni	327
Určování zdroje útoků	328
<b>TAKŽE?</b>	<b>329</b>

## **Kapitola 15**

### **VYŠETŘOVÁNÍ APLIKAČNÍCH SERVERŮ** **331**

<b>VYŠETŘOVÁNÍ INCIDENTŮ NA SERVERECH DNS</b>	<b>332</b>
Řešení přímých útoků	332
Vyšetřování zkorumpování vyrovnávací paměti	334
<b>VYŠETŘOVÁNÍ INCIDENTŮ NA SERVERECH FTP</b>	<b>335</b>
Řešení přímé kompromitace	335
Vyšetřování zneužití úložného prostoru	337
<b>VYŠETŘOVÁNÍ INCIDENTŮ SPOJENÝCH SE SLUŽBOU RPC</b>	<b>339</b>
<b>VYUŽITÍ ZÁZNAMŮ CHATOVACÍHO PROGRAMU PŘI VYŠETŘOVÁNÍ INCIDENTŮ</b>	<b>340</b>
<b>ŘEŠENÍ INCIDENTŮ SPOJENÝCH S BALÍKEM MICROSOFT OFFICE</b>	<b>341</b>
Hledání stop v dokumentech Office	341
Dešifrování dokumentů Office	342
<b>ZJIŠŤOVÁNÍ ZDROJE APLIKAČNÍCH ÚTOKŮ</b>	<b>344</b>
<b>OBNOVOVÁNÍ KOMPROMITOVANÝCH APLIKAČNÍCH SERVERŮ</b>	<b>345</b>
<b>TAKŽE?</b>	<b>346</b>

## **Kapitola 16**

### **VYŠETŘOVÁNÍ NÁSTROJŮ HACKERŮ** **347**

<b>JAKÝM ZPŮSOBEM JSOU SOUBORY KOMPILOVÁNY</b>	<b>348</b>
Statically linkované programy	348
Stripované programy	350
Programy zabalené pomocí UPX	351



<b>STATICKÁ ANALÝZA NÁSTROJŮ HACKERA</b>	<b>352</b>
Určení typu souboru	352
Revize řetězců ASCII a UNICODE	353
Online průzkum	356
Revize zdrojového kódu	356
<b>DYNAMICKÁ ANALÝZA NÁSTROJŮ HACKERA</b>	<b>357</b>
Vytvoření testovacího prostředí	357
Dynamická analýza systému Windows	366
<b>TAKŽE?</b>	<b>370</b>

## ČÁST 5

<b>DODATKY</b>	<b>371</b>
----------------	------------

### DODATEK A

<b>ZJIŠŤOVÁNÍ IDENTITY VE VIRTUÁLNÍM SVĚTĚ</b>	<b>373</b>
--	------------

<b>VYŠETŘOVÁNÍ ADRES IP</b>	<b>374</b>
Nslookup	374
Traceroute nebo tracert	376
Využití databáze Whois	378
Vyšetřování dynamických adres IP	382
<b>VYŠETŘENÍ ADRES MAC</b>	<b>388</b>
<b>STOPOVÁNÍ E-MAILU</b>	<b>391</b>
Stopování fakemailu	391
<b>VYŠETŘENÍ E-MAILOVÝCH ADRES, PŘEZDÍVEK, UŽIVATELSKÝCH JMEN A NÁZVŮ HOSTITELŮ</b>	<b>397</b>

### DODATEK B

<b>POLITIKA INFORMAČNÍHO ZABEZPEČENÍ A PŘÍPUSTNÉHO VYUŽITÍ</b>	<b>399</b>
--	------------

<b>OBLASTI POLITIKY INFORMAČNÍHO ZABEZPEČENÍ</b>	<b>400</b>
<b>POLITIKY PŘÍPUSTNÉHO VYUŽITÍ</b>	<b>401</b>
Ukázka politiky přípuštného využití	401

### DODATEK C

<b>ZODPOVĚDNÉ ORGANIZACE</b>	<b>403</b>
------------------------------	------------

<b>REJSTŘÍK</b>	<b>405</b>
-----------------	------------