

מדריך

Hacking

ואבטחת מידע

דורון סיון

מהדורה שנייה של הספר
"מדריך אבטחת מידע והגנה מפני האקרים"

שמות מסחריים

שמות המוצרים והשירותים המוזכרים בספר הינם שמות מסחריים רשומים של החברות שלהם. הוצאת הוד-עמי עשתה כמיטב יכולתה למסור מידע אודות השמות המסחריים המוזכרים בספר זה ולציין את שמות החברות, המוצרים והשירותים. שמות מסחריים רשומים (registered trademarks) המוזכרים בספר צוינו בהתאמה.

הודעה חשובה

קרא בעיון את המבוא לספר זה.

ספר זה מיועד לתת מידע אודות מוצרים שונים. נעשו מאמצים רבים לגרום לכך שהספר יהיה שלם ואמין ככל שניתן, אך אין משתמעת מכך אחריות כלשהי.

תוכן הספר וההפניות לספרים, לתוכנות, לאתרים ולמקורות מידע המוזכרים בו מסופקים "כמו שהם (as is)". השימוש בכל אלה הוא על אחריותו הבלעדית של המשתמש. הוצאת הוד-עמי והמחבר אינם אחראים כלפי יחיד או ארגון עבור כל אובדן או נזק ישיר או עקיף, אשר ייגרם, אם ייגרם, מהשימוש בספר ו/או בתוכנות ו/או באתרים ו/או כל מקור מידע או תוכנה המוזכרים בספר, ובכלל זה (רשימה חלקית): הפרעה במתן שירות, אובדן מידע, אובדן זמן, אובדן רווח וכד'.

המשתמש רשאי להשתמש בתוכנות המוזכרות בספר ו/או לפנות לאתרים ו/או למקורות מידע אחרים על אחריותו. כל אלה הם בבעלות ובאחריות החברות המייצרות, משווקות ומציגות אותם. הוד-עמי והמחבר אינם גובים תשלום עבור השימוש בתוכנות ובמידע ממקורות אחרים המוזכרים בספר. הוד-עמי והמחבר אינם מספקים תמיכה בהתקנה ו/או ההפעלה של התוכנות ו/או בגישה לאתרים ומידע אחר. מחלקת התמיכה בהוצאת הוד-עמי תגיש עזרה רק עבור מקרים של אי בהירות של הסבר בספר או שיבוש דפוס. כל שאלה לגבי תוכנה ו/או אתר ו/או מקור מידע כלשהם יש להפנות אל מפתח/יוצרי/משווקי התוכנה ו/או אל בעלי האתרים ו/או מקורות המידע.

הוצאת הוד-עמי והמחבר עשו כל מאמץ שתוכן הספר יהיה אמין ושלם. עם זאת, ההוצאה והמחבר אינם טוענים לאמינות ולשלמות של התכנים המוצגים בספר זה, ובמיוחד דוחים כל אחריות, ובכלל זה טענה להתאמה של הנאמר בספר למקרה ספציפי כלשהו. לא ניתן ליצור או להרחיב אחריות על ידי מידע שיווקי ו/או פרסומי כלשהו. ייתכן שההצעות ו/או ההמלצות הניתנות בספר לא יתאימו לכל מצב ומקרה. הספר משווק ונמכר תוך הבנה שההוצאה והמחבר אינם מספקים שירותים שונים הכרוכים בשימוש בספר, אלא לשם הבנת הכתוב ותיקון שיבושי לשון. לקבלת שירות מקצועי יש לפנות אל בעלי המקצוע בתחום. הן ההוצאה והן המחבר אינם אחראים לכל אובדן או נזק ישיר או עקיף, אשר ייגרם, אם ייגרם, מהשימוש בספר ו/או בתוכנות ו/או באתרים ו/או כל מקור מידע או תוכנה המוזכרים בספר. אין בכוונת ההוצאה ו/או המחבר להמליץ או להעדיף תוכנה ו/או אתר ו/או מקור מידע כלשהם. רק המשתמש הוא שיחליט כיצד לנהוג על פי המוצג בספר. המשתמש צריך להיות ער לעובדה שאתרי האינטרנט הינם דינמיים ועלולים להיסגר, לשנות את התכנים שלהם וכד'. ההוצאה והמחבר אינם אחראים לשינויים אשר עלולים לחול באתרים המוזכרים בספר, ועל כן להיות שונים ממה שהוצג בספר.

אין לעשות שימוש מסחרי ו/או להעתיק, לשכפל, לצלם, לתרגם, להקליט, לשדר, לקלוט ו/או לאחסן במאגר מידע בכל דרך ו/או אמצעי מכני, דיגיטלי, אופטי, מגנטי ו/או אחר - בחלק כלשהו מן המידע ו/או התמונות ו/או האיוורים ו/או כל תוכן אחר הכלולים ו/או שצורפו לספר זה, בין אם לשימוש פנימי או לשימוש מסחרי. כל שימוש החורג מציטוט קטעים קצרים במסגרת של ביקורת ספרותית אסור בהחלט, אלא ברשות מפורשת בכתב מהמוציא לאור.

מדריך

Hacking

ואבטחת מידע

דורון סיון



עריכה ועיצוב: שרה עמיהוד, יצחק עמיהוד

עיצוב עטיפה: שרון רז

לשם שטף הקריאה כתוב ספר זה בלשון זכר בלבד. ספר זה מיועד לגברים ונשים כאחד ואין בכוונתנו להפלות או לפגוע בציבור המשתמשים/ות.

(C)

כל הזכויות שמורות

הוצאת הוד-עמי בע"מ

ת.ד. 6108 הרצליה 46160

טלפון: 09-9564716

דואר אלקטרוני: info@hod-ami.co.il

אתר באינטרנט: www.hod-ami.co.il

הודפס בישראל ספטמבר 2011

All Rights Reserved

HOD-AMI Ltd.

P.O.B. 6108, Herzliya

ISRAEL, 2011

מסת"ב 978-965-361-386-7 ISBN

**הספר מוקדש בחום ואהבה לאשתי דליה
ולילדיי עופר, נעה ועמית**

תוכן עניינים מקוצר

19.....	הקדמה
23.....	פרק 1: מבוא - מושגים בתקשורת ואבטחת מידע
79.....	פרק 2: Hacking
249	פרק 3: כלי תקיפה מתקדמים
265	פרק 4: Check Point Firewall - NGX
325	פרק 5: Microsoft Firewall - Forefront
371	פרק 6: גישות ומודלים בתחום אבטחת המידע
415	אינדקס

תוכן העניינים

19	הקדמה
20	כיצד ניתן להתגונן בפני Hacking?
21	מבנה הספר
23	פרק 1: מבוא - מושגים בתקשורת ואבטחת מידע
25	מודל שבע השכבות
26	השכבה הפיזית
26	טופולוגיות פיזיות
26	Star
26	Mesh
27	ציוד תקשורת
27	ציוד לחיבור ברשת
27	ציוד לחיבור בין רשתות
27	חיווט
28	זוג שזור – (Twisted Pair) TP
29	סיב אופטי
29	תקשורת אלחוטית
29	רכוזת – Access Point
29	עמדות
30	נתבים
30	שכבת עורק הנתונים – Data Link Layer
31	כתובת פיזית
32	שכבת הרשת
32	כתובות לוגיות – Logical Network Address
34	שיטות ניתוב
37	שכבת התעבורה – Transport Layer
41	שכבת השיח – Session Layer
41	שכבת התצוגה – Presentation Layer
42	שכבת היישום – Application Layer

42	סיכום מודל שבע השכבות
44	Ethernet תשתיות Ethernet
44	Ethernet מבנה המנה ב-
45	רכוזות
46	תקן 802.1X
48	רשתות מרחביות (WAN)
48	קו נל"ץ (נקודה לנקודה) – Point to Point
48	טכנולוגיות לחיבור משתמשים לאינטרנט
48	ADSL
49	טכנולוגיית כבלים
49	נתבים – Routers
51	נתבי ADSL
51	נתבי CISCO
51	User EXEC Mode
52	Privileged EXEC Mode
52	Global Configuration Mode
52	Interface Configuration Mode
53	Line Configuration Mode
53	Router Configuration Mode
54	כללי
54	עדכון נתבים
54	ניתוב דינמי
55	RIP
55	OSPF
55	ניתוב סטטי
56	שימוש ב-Sniffer
58	מודל Internet
59	פירוט היישומים במודל
59	שכבת היישום
59	הפרוטוקולים השייכים לשכבת היישום
59	השכבה Host to Host
60	השכבה Internet
61	שכבת הגישה לרשת
61	כתובות IP
61	Class A

62Class B
62Class C
63 (Subnet Mask) מסכת תת-רשת
63 Default Gateway
64 השימוש בכתובות פנימיות
65 IPSec
67 מהו Tunnel?
69 VPN
72 SSL
73 Simple Network Management Protocol – SNMP
73 הגדרת סוכן SNMP
74 סיכום מושגים ושרתים
74 IP Address
74 Subnet Mask
74 Default Gateway
75 DNS
75 HOSTS
75 WINS
76 DHCP
76 רשימת פקודות
76 PING
76 ARP
76 NETSTAT
77 NBTSTAT
77 IPCONFIG
77 TRACERT
77 ROUTE
77 NSLOOKUP

79..... פרק 2: Hacking

81 סקירה ראשונית
81 בעיות הקשורות לשכבה הפיזית
85 בעיות הקשורות לשכבת עורק הנתונים
94 התקפות בנושא Switch
99 בעיות הקשורות לשכבת הרשת

102	Hacking מול נתבי Cisco ומנגנון SNMP
105	סניפרים (Sniffers)
109	בעיות הקשורות לשכבת התעבורה
115	SNMP
120	בעיות אבטחה הקשורות לשכבות 5-7 של מודל השכבות
120	סיסמאות
121	תוכנות לפריצת סיסמאות
128	שימוש במאגרי סיסמאות
130	פריצת סיסמאות של קבצים
131	הצפנות ברשת
134	סיכום מודל השכבות
135	איסוף מידע על הארגון
146	איסוף מידע ופגיעה ברמת רשת
146	כלי איתור של צמדות ושירותים
148	כלים לפגיעה בשירותים
150	ביצוע תקיפות מסוג MITM
151	Hacking על מערכות הפעלה
151	Windows
156	סיכום ודרכי התגוננות
157	Linux
157	פקודות שכיחות
157	פקודות הקשורות למשתמשים
158	פקודות הקשורות למערכת הקבצים
165	סיכום ודרכי התגוננות
166	Services
166	תקיפות שמבוססות על Social Engineering
169	דרכי פגיעה בשרתי Windows ואופן התגוננות
169	דרכי פגיעה ודרכי הגנה על שרת DNS
175	הכרטיסייה Forwarders
175	הכרטיסייה Advanced
177	הכרטיסייה Root Hints
178	הכרטיסייה Security
179	היכן כדאי למקם שרת DNS?
181	שילוב בין שרת DNS לבין שרת DHCP
183	שרת IIS

184	Web Site	הכרטיסייה
185	Directory Security	הכרטיסייה
185	Authentication and access control	
186	IP address and domain name restrictions	
187	Secure communications	
188	Home Directory	הכרטיסייה
189	domain	בקר
193		הקשחת שרתים
193	Windows 2000/2003	שרת
193	Windows 2008	שרת
194	SQL	שרת
194	IIS	שרת
195	(Security Configuration Wizard) SCW	שימוש בכלי
196	Exchange	נקודות למחשבה בשרת דואר
199		ניצול פרצות בתוכנה
203		עבודה דרך שורת הפקודה
205	Processes-	לב ל-תשומת
207	(Spy)	וירוסים ותוכנות ריגול
207		מהם וירוסים?
208		הנזק הנגרם למחשב
208		התמודדות עם וירוסים
209		התמודדות עם וירוסים חמקנים
211		התמודדות עם סוסים טרויאנים
211	Spy	התמודדות בפני פריצות למחשב ותוכנות
217	Spy	תוכנות
218		דוגמאות לשימוש בתוכנות סמויות
222		מציאת הקשר בין יישומים שרצים במחשב לבין פורטים פתוחים
223	Internet Explorer	ב- הגדרות אבטחה
223		הכרטיסייה התקשוריות
225		הכרטיסייה מתקדם
225		הכרטיסייה תוכן
226		הכרטיסייה כללי
227		הכרטיסייה אבטחה
228		הצפנה
228		פרטיות

230	שלמות
230	פונקציית ערבול (hash)
232	נוהל עבודה של אלגוריתם RSA
234	אימות
234	ניהול מפתחות מרכזי במערכת אסימטרית
235	נוהל עבודה עם אלגוריתם סימטרי
235	שימוש משולב בשתי הטכנולוגיות
237	סוגי התקפות
237	סיסמאות
241	אימות באתרי אינטרנט
245	SQL Injection
246	לימוד המערכת
246	שלב המטרות
247	Google Hacking

פרק 3: כלי תקיפה מתקדמים

249	סקירת כלי תקיפה - BlackMoon 2.0
252	פירוט כלים לפי קטגוריה
252	הקטגוריה Enumeration
252	Dnsmap
252	Dnswalk
252	Googmail
252	Metagoofil
252	Snmpenum
253	הקטגוריה Scanning
253	Nmap
253	Hping
253	Arping
253	P0f
253	הקטגוריה Vulnerability analysis
253	Impacket-smbclient
254	Impacket-rpcdump
254	Impacket-samrdump
254	Cisco-Global-Exploiter
254	Cisco-Auditing-Tool

254	Database analysis	הקטגוריה
254	Mysqlaudit	
254	Sqlmap	
254	Sqlninja	
255	Website analysis	
255	Asp-audit	
255	Burpsuite	
255	Dirbuster	
255	Nikto	
255	Wapiti	
255	Xss	
255	Exploiting	הקטגוריה
256	Msfconsole	
256	Password Cracking	
256	Bkhive	
256	John	
256	Ophcrack	
256	RainbowCrack	
256	Bruteforce	
256	Brutessh	
257	Tftp-bruteforcer	
257	Vncrack	
257	Spoofing & Sniffers	הקטגוריה
257	Ettercap	
257	Wireshark	
258	WEP-Cracking	מסוג תקיפות
261	SQL Injection	מסוג תקיפות
262	(Penetration test)	בדיקות פריצה
264	סקירה קצרה על לינוקס	
265	Check Point Firewall - NGX	פרק 4
266	(Packet)	נוהל בדיקת מנה
268	Packet Filter	– דור ראשון
268	Proxy Gateway	– דור שני
269	Stateful Inspection	– דור שלישי

271	מבנה המערכת.....
271	Single Gateway Product.....
272	Enterprise Management Product.....
273	התקנה של המערכת בלינוקס.....
274	התקנה ב-Windows.....
275	הכרת תפריטי הניהול.....
275	Network Objects.....
275	Services.....
275	Resources.....
276	Servers and OPSEC Application.....
276	Users and Administrators.....
276	VPN Communities.....
277	יצירת Rules (חוקים).....
281	זמני פעולה.....
282	מעקב.....
282	קביעת אובייקטים.....
283	יצירת אובייקט שייצג רשת.....
283	יצירת אובייקט שייצג שרת.....
284	הגדרת אובייקט שייצג Firewall.....
286	2 חוקי החובה ואופן התקנת ה-Rules.....
286	חוקי החובה.....
287	בדיקה והתקנה.....
289	ניהול מעקב ובקרה.....
289	LOG.....
292	Check point configuration.....
294	License.....
294	ניהול הגדרות המערכת.....
295	NAT - תרגום כתובת IP פנימית לכתובת חיצונית.....
296	כיצד להגדיר זאת?.....
298	שילוב עם Active Directory.....
301	הגנה על תוכן.....
301	SmartDefense.....
302	Web Intelligence.....
304	תוספות בגרסת R70.....
306	OPSEC.....

309	סינון על סמך קובץ שיוצרים מראש
310	חיבור VPN
310	Remote-access VPNs
311	נוהל ההגדרה
313	Intranet VPNs
317	Safe@Office (SBox)
321	תפריטי Network
322	חיבורי VPN
323	UTM 1 Edge

פרק 5: Microsoft Firewall (ISA) Forefront

327	אופן השימוש ב-Forefront
327	נקודת הקישור בין הארגון לבין האינטרנט
328	נקודת הקישור בין סניפים
328	התקנת המערכת
329	מהלך ההתקנה
329	ומה לאחר ההתקנה?
330	סוגי לקוחות
331	פתרון אבטחה כולל
334	גישה מרוחקת ל-ISA וגייביים
334	אפשר גישה מרוחקת
335	יצירת Rules והגדרות
336	הגדרת Access Rules
337	פירוט סדר הפעולות
344	אופן בקרה על זרימת המידע ב-Firewall
346	כיצד פועלת מערכת IDS ב-ISA?
346	מערכת המעקב אוספת מידע לפי פירוט זה
346	בקרה ברמת שכבה שלישית (IP) ורביעית (TCP, UDP)
347	בקרה ברמת היישום
347	כיצד נגדיר זאת ב-ISA?
349	System Policy
351	גישה מבחוץ לאתרים פנימיים
353	שרת הדואר Exchange
356	סינון ואבטחה לשירות HTTP
358	אישור או מניעת תנועה לפי החתימה Signature

360VPN
360 סוגי החיבור ב-VPN
364ניטור ובקרה
366Forefront בגרסת HTTP ברמת
367סינון תעבורה משופרת
369מערכת IPS/IDS

פרק 6: גישות ומודלים בתחום אבטחת המידע 371

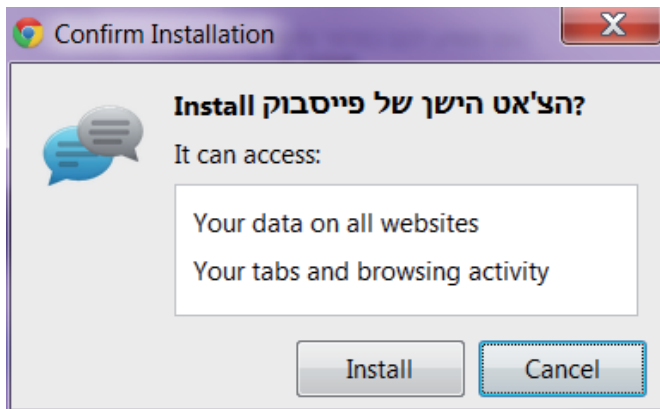
375 כלל ראשון – נסה לחשוב כהאקר
375 דברים שניתן לעשות ברמת הרשת
375 דברים שניתן לעשות ברמת Host
376 פגיעה ברמת היישום
376 כלל שני – היערך בהתאם
376 הגנה על יישומים
377 הגנה על Host
378 הגנה ברמת הרשת
379 מהם השיקולים ברכישת Firewall?
380 כיצד ליצור אבטחה ברמת יישום
381 Threat Model
382 מודל Stride
383 מהם הכלים שישמשו אותנו להערכת הסיכונים
384 כלים טכנולוגיים לאבטחת מידע מאוחסן ומידע שעובר ברשת
384 כלים טכנולוגיים לאבטחה בעת העברת מידע
385 דרכי התמודדות מול Hacking ברמת יישום
385 Cross-Site Scripting
388 Buffer Overflow
390 SQL injection
391 דרכים לטיפול בבעיות אבטחה ביישומים
394 אבטחה מומלצת עבור Intranet
395 Integrity
395 Authentication
395 Authorization
395 אבטחה מומלצת עבור Extranet
396 חיבור בין אתרים שונים, לדוגמה חברות שונות למטרות B2B
396 חיבור בין משתמש לבין אתר החברה

397	אבטחה מומלצת עבור Internet
398	תכנון מבנה רשת שכוללת שרתי דואר, Web ואנטי וירוס
400	ריכוז שיטות פריצה (Hacking) וכלי הגנה, בהתאם למודל 7 השכבות
401	אתרים חשובים
402	פעולות במקרה של פריצה או פגיעה במידע
402	בדיקות שיש לעשות כאשר יש חשש לחדירה לארגון
404	בדיקות בעזרת מוצרים קיימים
404	MBSA
407	GRC
408	פגיעה במידע עקב וירוסים, או נזק ממקור חיצוני דוגמת שריפה
409	גניבת מידע פנים ארגוני על ידי עובד מתוסכל
411	קריסת שרתים, שירותים או קווי תקשורת באופן שמונע את המשך הפעילות
412	מודלים ונהלים בתחום אבטחת מידע
412	תקן ISO 27001
415	אינדקס

הקדמה

בתחילת ההקדמה ברצוני להציג מספר ידיעות שהופיעו בשנה האחרונה מהאתר של globes בדבר פריצות לאתרים, ארגונים, בנקים ומחשבים אישיים פרטיים לשם השחתה וגניבת מידע רגיש.

עולם אבטחת המידע, הולך ומשנה את פניו. האקרים מבצעים כיום מגוון פעילויות וחלקן אף על בסיס אידיאולוגי, פוליטי וכלכלי. אתחיל בסקירת כתבות הונאת פייסבוק חדשה בדמותה של הודעת Pop-Up בעברית, המציעה לגולשים להחזיר את ממשק הצ'אט של פייסבוק למצב הקודם שלו.



בהודעה המוצגת בפני הגולש מופיעה השאלה: "האם להתקין את הצ'אט הישן של פייסבוק?" בתוספת לחצן "ביטול" ולחצן "התקן". ברגע שהגולש נותן את הסכמתו להתקנה של הצ'אט החדש, כביכול, הוא מועבר לדף חדש המציע לו להוריד תוסף לדפדפן כרום FB Old Chat, ובהתקנת התוסף המשתמש מאפשר לגורם הזדוני שעומד מאחורי ההונאה הזו גישה לפרופיל הפייסבוק שלו, למידע פרטי עליו וכן לנתוני הגלישה של המשתמש ברשת.

פריצה אחרת מ-2011/9 (מתוך גלובס באינטרנט) - "האקרים טורקיים ופרו-פלסטינים פרצו לשרת ניתוב DNS ישראלי, שאיפשר להם לפגוע במשך שעות במאות אתרים ישראליים. בין האתרים שנפגעו: מיקרוסופט ישראל, מועצת העיתונות, קוקה קולה ישראל ו-MSN-ישראל".



מתוך הכתבה - "האקרים טורקיים פרצו לשרת ניתוב DNS ישראלי, שאיפשר להם לפגוע במאות אתרים ישראליים. מתקפת ההאקרים החלה למעשה כבר ביום שבת, כשבשעות האחרונות המתקפה המתוכננת רק מחריפה כחלק מההסלמה המדינית בין ישראל לטורקיה.

מתקפות ההאקרים על אתרי אינטרנט ממשלתיים, וכן סוכנויות ביון מהמובילות בעולם, ממשיכות להסלים. האקרים, ככל הנראה איראנים, הצליחו לפרוץ לאתרי האינטרנט של סוכנויות הביון הגדולות בעולם, בהן המוסד הישראלי, ה-CIA האמריקני וגם ה-MI6 הבריטית.

הפריצה התאפשרה בעקבות פריצה אחרת שהתרחשה לפני כחודשיים, לשרתי חברת האבטחה ההולנדית DigiNotar המנפיקה תעודות אבטחה לאתרי אינטרנט (SSL) המאפשרות חיבור מאובטח בין אתרים ברשת. באירוע הזה נלקחו למעלה מ-500 תעודות של אתרים שונים, ביניהן כאלו שאיפשרו להאקרים להתחזות לאתרים מאובטחים מול אתרי האינטרנט של גופי הביון ולמעשה לקבל את אמונם ולחדור לתוכם."

כיצד ניתן להתגונן בפני Hacking?

תחילה חשוב להבין כי ללא ידע מספיק ב-Hacking, לא ניתן לבצע הגנה טובה. כדי להתגונן בפני פורצי מחשב, האקרים (Hackers), עליך להכיר היטב את דרך פעולתם. מסיבה זו, הקדשתי חלק נרחב מספרי לנושא הפריצה למחשבים ולאיתרים ולדרכי התקיפה של ההאקרים. המידע בספר זה אינו מיועד ללמד אותך לפרוץ למחשבים ולאיתרים, אלא לעזור לך לפתח מערך הגנה עמיד בפני ההאקרים. פריצה למחשבים ואיתרים מהווה עבירה על החוק הישראלי ודינה מאסר. רוב מעשי הפריצה ניתנים למניעה בקלות. תחילה עליך לדעת ולהבין כיצד תוקפים אותך כדי למצוא דרכים להתגונן בדרך הנכונה. עליך ליצור מערכת

התגוננות יעילה ואפקטיבית ולא להתגונן מתוך פחד בדרכים יקרות ולא מתוחכמות. במילים אחרות עליך ללמוד כיצד להתגונן נכון. Firewall (קיר אש, חומת אש) לברו אינו מספיק כדי להגן על המערכת. הוא צריך להיות מרכיב אחד במכלול מערכת האבטחה, כפי שיצרני ה-Firewall חוזרים ומדגישים.

לא צריך להרים ידיים נוכח הפריצות המתרחשות בכל יום בחברות טכנולוגיות מובילות ובאתרים פרטיים.

מבנה הספר

בעזרת ספר זה תלמד על סוגי הפריצה האפשריים למחשבים ולאיתרים, כאלה שראית בדוגמאות שהצגתי, ורבים נוספים. וחשוב מכך - תלמד כיצד להתגונן מפניהם ביעילות ולפתח מערך אבטחה עמיד ואפקטיבי.

בספר 6 פרקים:

1. מבוא לרשתות ואבטחה.
2. פריצה (Hacking) בכל הרמות.
3. כלי תקיפה מתקדמים.
4. לימוד מקצועי של NGX - Check-point Firewall.
5. לימוד מקצועי של ISA - Microsoft Firewall.
6. פרק סיכום המספק כלים לבניית הגנה חכמה בארגון. בעזרת כלים אלה תלמד להתמודד מול סוגי פריצה שונים, החל מרמת התשתית ועד רמת היישום בבית ובארגון.

מומלץ לקרוא בעיון את הפרקים העוסקים ב-Firewall. בפרקים אלה תלמד כיצד ההאקרים מנסים להתמודד עם מחסום ה-Firewall, תכיר את גישות האבטחה השונות שהחברות נוקטות בהן, וגם תוכל לבחור את מנגנון ה-Firewall המתאים לך ביותר.

קוראים המעוניינים לשלוח הערות, מוזמנים לפנות לכתובת:

dsivan@sivanet.co.il

בתקווה שתהנה מקריאת הספר ותפיק ממנו תועלת,

דורון סיון

ספר זה שייך לסדרה בת שלושה ספרים:

"מדריך חומרה ותוכנה לטכנאי PC", מהד' 5 (2011)

"מדריך רשתות לטכנאי PC ולמנהלי רשת", מהד' 4 (2011)

"מדריך Hacking ואבטחת מידע" (ספר זה)

בספר תמצא הפניות לספרים בשם מקוצר: "מדריך חומרה" ו"מדריך רשתות". הכוונה לספרים המפורטים כאן, כולם בהוצאת הוד-עמי.

1

מבוא

מושגים בתקשורת ואבטחת מידע

פרק זה חיוני להבנת שאר הפרקים, מכיוון שהפריצה (Hacking) מבוצעת דרך אמצעי תקשורת דוגמת האזנה למידע שזורם ברשת, פריצה למחשב דרך פורטים (ports) פתוחים ועוד. על כן, אינך יכול ללמוד את נושא הפריצה למחשבים ללא ידע סביר ברשתות.

נושא התקשורת רחב מאוד וכולל מושגים רבים. פרק זה יספק לך כלים להבנת מודל שבע השכבות (OSI). הדיון יכסה את כל תחום התקשורת באופן כללי, ויהיה תיאורטי במידה רבה. נתחיל בשאלה מדוע אנו זקוקים לרשת תקשורת, ובהמשך נסקור את מודל שבע השכבות, נכיר את פרוטוקול TCP/IP ואת ציוד התקשורת הנפוץ. החומר בפרק זה אינו מיועד להכרת נושא הרשתות ברמה של מנהל רשת. החומר מובא במטרה לספק ידע ברמה הדרושה, כך שמי שאינו מתמצא בתחום, יוכל להבין את הפרקים הבאים.

נתחיל מהכרת המושג רשת תקשורת. אני נוהג לתאר רשת תקשורת כחיבור של שני מחשבים לפחות, למטרת שיתוף משאב כלשהו, כגון: מדפסת או שרת קבצים.

כדי לקיים רשת, המחשבים צריכים לתפקד באחד משני המצבים הבאים:

(1) **Server** – שרת, עמדה המספקת שירותים לעמדות קצה.

(2) **Client** – לקוח, הכוונה לעמדת קצה שמבקשת ומקבלת את השירותים מהשרת.

אם כן, ניתן להבין באופן אינטואיטיבי שרוב ההתקפות של ההאקרים נעשות כלפי מחשבים המתפקדים כשרתים, מכיוון שהם מכילים את הנתונים והמידע שאותו רוצים לחשוף. עם זאת, נוכל לראות לעתים התקפות מתוחכמות שבהן גורמים לעמדות לבצע התקפות מרוכזות על השרתים כדי לשבש את אופן פעולתם.

מהם התנאים להיווצרות רשת?

(1) שירותי רשת

מדוע יש צורך ברשת? בדרך כלל הרשת מיועדת לשיתוף משאבים בארגון, כמו מידע או ציוד. ברור שכל מחשב שמספק שירותי רשת מהווה יעד לגיטימי להתקפות עליו, או להתקפות דרכו על יעדים נוספים. הסיבה לכך היא שמחשב כזה מתוכנן לספק שירות ולענות לבקשות שמגיעות מלקוחות, ולכן ניתן לנצל זאת ולגרום לו לספק מידע רב מדי, או להציף אותו בבקשות עד שיקרוס.

(2) פרוטוקול תקשורת

הפרוטוקול הוא אוסף הכללים לפיהם מועברים הנתונים ברשת, כמו לדוגמה פרוטוקול TCP/IP. הבחירה בפרוטוקול זה אינה מקרית. בפרוטוקול זה משתמשים באינטרנט וכתוצאה מכך גם ברוב הרשתות בעולם. פרוטוקול TCP/IP לא תוכנן במקור להתמודד עם האקרים, ולכן הוא פרוץ כמו רשת דייגים. בהמשך תלמד להשתמש בפרצות וגם לנסות לסגור אותן.

(3) ציוד תקשורת

הציוד הינו המדיה, תווך התקשורת, בעזרתו מועברים שידורי הרשת. הציוד כולל: סוגי חיווט, רכזות וסוגי רשתות.

רשתות התקשורת מסווגות לשני סוגים עיקריים:

(1) LAN (Local Area Network)

רשת תקשורת מקומית. רשתות תקשורת מקומיות מוגבלות לטווחי פעולה קצרים, עד מספר קילומטרים. דוגמה לרשת מסוג LAN היא רשת Ethernet המצויה במשרדים.

(2) WAN (Wide Area Network)

רשת מרחבית. רשתות תקשורת מרחביות מתפרסות על פני שטחים נרחבים ואפילו על פני כל כדור הארץ (למעשה, הן אוסף של רשתות מסוג זה). דוגמה לרשת בין אתרים היא ATM.

ייתכן שברגע זה התמונה נראית מעורפלת מעט, אולם תחשוב על מה שמתרחש בעת שאתה גולש ב-Internet. לביצוע הפעולה דרושים שלושה "שותפים":

- ⊙ ציוד תקשורת – מודם המחבר את התשתית של חברות פרטיות וציבוריות.
- ⊙ פרוטוקול תקשורת – TCP/IP.
- ⊙ שירותי רשת – הורדת קבצים ותוכניות, קבלה ושליחה של דואר אלקטרוני על ידי תוכניות דוגמת הדפדפן, שפונות אל השרת ומביאות ממנו נתונים ומידע.

מודל שבע השכבות

כדי לקיים תקשורת בין מחשבים, יש לענות על שלושה תנאים:

- 1) רצון וצורך לשתף נתונים (מידע) וציוד.
- 2) הקמת תשתית חיווט (פיזית או אלוטית), כדי לאפשר את מעבר המידע.
- 3) קביעת כללים שיאפשרו תקשורת אמינה.

כדי לאפשר זאת בצורה פתוחה ולא להיות כבולים לחברה מסוימת כלשהי, נוצר מודל **OSI**. זהו מודל "פתוח" – הקוד שלו אינו שייך לחברה כלשהי. במודל נקבעו דרכי העברת המידע ברשת, וכל ספק צריך ליישם את המודל והתקנים במוצרים שלו. בזכות מודל זה ניתן להרכיב רשת המתבססת על מוצרים של חברות שונות. מודל OSI מבוסס על **שבע השכבות**, כאשר לכל אחת מהן תפקיד מוגדר. חלק מהשכבות עוסקות ברמה הפיזית, כמו לדוגמה סוג שידור. חלק מהן עוסקות באופן מעבר המידע ברשת, כמו לדוגמה איתור המחשב, וחלק מהן עוסקות באופן הגישה למידע שנמצא בשרת.

כל שכבה יוצרת קשר רק עם השכבות הצמודות אליה: זו שמעליה וזו שמתחתיה. בצד השולח: כל שכבה מקבלת מידע מהשכבה שמעליה, מבצעת עיבוד מסוים, מוסיפה את כל המידע בצירוף הכותרת ומעבירה אל השכבה שמתחתיה. כאשר המידע מגיע לשכבה התחתונה ביותר, הוא מועבר אל אמצעי חיווט המעבירים אותו אל מחשב היעד. במחשב היעד המידע זורם בכיוון "מעלה", כאשר כל שכבה "מקולפת" מהמידע שהתווסף לה בזמן השידור. השכבה המקבלת זהה לשכבה האורזת את המידע למשלוח.

בפרק Hacking אסביר כיצד ניתן לפרק את המעטפת (frame) ולשייך כל סוג תקיפה לשכבה המתאימה. לדוגמה, לימוד מידע באמצעות גילוי פורטים פתוחים מתייחס לשכבות 4 ומעלה, התקפות על כתובת IP משויכות לשכבה 3, וכך הלאה. בדרך זו תוכל להתמודד עם שפע סוגי התקיפות ותוכל לבנות מודל הגנה טוב יותר. נסקור בקצרה את השכבות ותפקידיהן במערך התקשורת.

2

Hacking

פרק זה נמצא לאחר פרק המבוא העוסק במושגי תקשורת ואבטחת מידע, ולפני לימוד Firewall, ולא בכדי. יש להכיר היטב את נושא רשתות התקשורת כדי להבין פרק זה במלואו, שכן בפרק זה ניכנס לנעליו של האקר ונלמד על דרכי פעולתו תוך שימוש במושגים מהפרק הראשון.



כדי להבין לעומק את דרכי התקיפה של ההאקר, תכיר בפרק זה כלי Hacking שונים. ללא היכרות זו לא תוכל לטפל כראוי בתקיפות של האקרים. זו אינה קלישאה, אנשי IT המנסים להתמודד עם האקרים בעזרת כלים של אנשי IT בלבד, וללא הקצאת זמן הולם למטרה – מתקשים לעמוד במשימות ההגנה. מטרת פרק זה אינה להפוך אותך להאקר, אלא להציג



בפניך שלל כלים המשמשים האקרים, כדי שתהיה מודע לכך שבסבירות גבוהה מאוד אינך מוגן כנדרש. בהמשך יוצגו בפניך מגוון כלים של האקרים, כולל הדגמות והפניות ספציפיות, זאת כדי לגרום לך לנסות ולחשוב אחרת בנושא אבטחת המידע. התפיסה שעומדת בבסיס פרק זה היא, שתשתמש בכלים אלה למטרות חיוביות לארגונך, דבר שמכונה **Ethical Hacker**.

בוודאי כבר למדת על מודל שבע השכבות. המודל מתחיל מהשכבה הפיזית ומגיע עד שכבת היישום. גם כאן נעסוק בנושא האקינג לפי מודל זה. תחילה נסקור בעיות אבטחה ברמה הפיזית דוגמת השראות. נמשיך לשכבה השנייה בה נכיר התקפות בנושא כתובות MAC והאקינג על Switch. בשכבה השלישית נכיר את הנתב וההתקפות עליו, כולל סריקת כתובות IP כמובן. בשכבה הרביעית נכיר התקפות מבוססות TCP, ולסיום נכיר התקפות ברמת סיסמאות, גניבת מפתחות הצפנה, SQL Injection וניצול Buffer Overflow ביישומים.

כלל ידוע הוא, שכדי להתגונן היטב חובה להכיר את כלי התקיפה. בהמשך הפרק אציג את כלי התקיפה בפירוט רב. רק זכור שהמטרה היא ללמוד להתגונן. כמו כן עליך לשנן את הנקודה החשובה הבאה: רק כשליש מניסיונות התקיפה מגיעים מבחון. רוב ניסיונות התקיפה הם פנים ארגוניים, כלומר על ידי עובדים של הארגון או מי שמורשים להיכנס למחשבים של הארגון. התעלמות מנקודה חשובה זו גורמת לך לבנות חומות הגנה לא יעילות.

בפרק זה נתמקד בפעולות התקיפה של ההאקר. בפרקים שעוסקים ב-Firewalls נלמד כיצד הם מסייעים לך בהתמודדות עם תקיפות, ובפרק הסיכום נלמד כיצד להיערך ברמה הארגונית לתקיפות פנים וחץ ארגוניות.

כדאי לזכור שאבטחת מידע מתחלקת למספר קטגוריות:

- ⊙ אבטחה ברמת תשתיות התקשורת - ציוד תקשורת.
- ⊙ אבטחת ברמת system - שרתים, תחנות קצה.
- ⊙ אבטחת מידע ברמת האפליקציה - penetration tests, כתיבת אפליקציות מאובטחות, חקירת פשעי מחשב.

בפרק תהיה התייחסות לרוב המרכיבים, וכל אחד מהקוראים יתמקד בנושאים הרלוונטיים עבורו.

שם לב שהפרק מכיל מידע רב למעוניינים לעבור הסמכת **CEH** - Certified Ethical Hacker.

מבנה הפרק - בפרק משולבים שני חלקים חשובים בעבוד ההאקר:

- ⊙ איסוף מידע (fingerprinting) על היעד. לכך קיימים כמובן מגוון שיטות, החל מאיסוף מידע על היעד, דרך אתר האינטרנט, facebook, דוא"ל ועד סריקת פורטים ועוד. בחלק זה נכיר מגוון כלים דוגמת: LAN Scanner, nmap, כלים חזקים שנעזרים ב-Google ומגוון דרכים לפריצת סיסמאות דוגמת: Aircrack.
- ⊙ ביצוע Hacking על היעד. לאחר שנאסף המידע, מגיע שלב שבו נחפש פגיעויות (vulnerability) במערכות שנסקרו. כאן נכיר את metasploit שיסייע לנו לנצל ולהשתמש ב-exploits (כלי חדירה) מוכנים.

בפרק יש התייחסות לנושאים הבאים:

- | | | |
|---------------------|-----------------------|-----------------------------|
| ⊙ Foot printing | ⊙ Sniffers | ⊙ SQL Injection |
| ⊙ Scanning Networks | ⊙ Social Engineering | ⊙ Cryptography |
| ⊙ Enumeration | ⊙ Denial of Service | ⊙ Hacking Wireless Networks |
| ⊙ System Hacking | ⊙ Hacking Web servers | |

סקירה ראשונית

בעיות הקשורות לשכבה הפיזית

כיוון שהשכבה הפיזית עוסקת בתשתיות, נתמודד בפרק זה עם תשתית לא מאובטחת, כגון חוטי נחושת ותקשורת אלחוטית.

לגבי חוטי נחושת, מכיוון שזרם חשמלי העובר בקו נחושת יוצר שדה מגנטי סביבו, ניתן לחבר ציוד מתוחכם בקרבת הכבל שיפענח את האותות העוברים, בזכות ההשראה הנוצרת סביב הכבל.

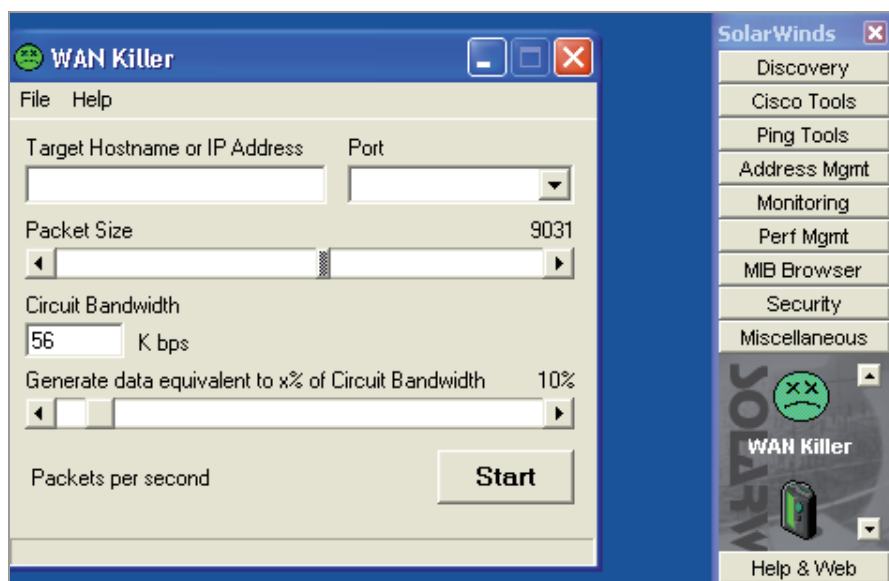
לספקנים מביניכם – חשבתם פעם מדוע מהירות המחשב אינה זהה בכל? מדוע המעבד כה מהיר אך מעבר המידע בלוח האם ובכרטיסים איטי יותר? הסיבה היא שלא ניתן לשדר בתדרים כה גבוהים דרך חוטי נחושת, מכיוון שעקב ההשראה הגבוהה חוטי הנחושת יפריעו אחד לשני. אותה השראה משמשת גם את אלה המעוניינים להאזין למידע, לכן במקומות מאובטחים משתמשים בסיבים אופטיים. לסיב זה אין השראה, כיוון שהמעבר הוא של קרני אור ולא של אותות חשמליים. בנוסף, לא ניתן לנתקו ולחבר אלמנט נוסף מבלי שזה יורגש מייד.

כמובן שאין טוב בלי רע, ומחיר התקנת סיב אופטי עשוי להרתיע אותך. שקול התקנה של הסיב בין מקומות אסטרטגיים.

תקשורת אלחוטית והטיפול בה, אלה נושאים מורכבים יותר. הוזלת המחירים ביחד עם שיפור עוצמת השידור, העלתה את שכיחות השימוש בה. עם זאת, מנהלי הרשת עדיין חוששים בצדק מהרעיון שאנטנה מרכזית משדרת לסביבה, וכל מי שנמצא בתחום יכול עקרונית לנסות ולהתחבר אליה.

תופעת לגלות כמה פשוט וקל לגרום לנזק משמעותי ברמת התשתית. לדוגמה, התוכנה הבאה (WAN Killer) גורמת לעומס ברמת WAN על ידי יצירת תעבורה רבה. לאחר שמקלידים את כתובת היעד והפורט המבוקשים, ואת גודל המנה (Packet) אשר תופנה ליעד, ניתן לקבוע בחלק התחתון של המסך איזה יחס מרוחב הפס של הרשת אתה מעוניין שהתוכנה תתפוס.

קיימים התקנים שמתחברים לשקע המחשב וממוקמים בין תקע הכבל שמגיע מהשרת לבין השקע במחשב. במצב זה כל התעבורה דרך ההתקנים האלה משודרת באופן אלחוטי לסביבה הקרובה וניתן להאזין לה.



בעיה נוספת שקשורה במיוחד לשימוש ברשת אלחוטית, היא יכולת האזנה קלה גם בדרך שונה מזו שהוזכרה למעלה, והדברים ידועים ומוכרים. היתרון של שימוש ברשת אלחוטית



גורר עימו כמובן בעיות לא מעטות, כשהחמורה שבהן נעוצה בעובדה שכל מי שנמצא בטווח של המשרד מסוגל לקרוא נתונים ואף לשלוח מידע דרכה. מספר תוכנות שמסייעות במיוחד לביצוע **Sniffer** ברשת אלחוטית, הן:

- ⊙ Kismet (למערכת הפעלה לינוקס).
- ⊙ Aircrack-ng (למערכת הפעלה לינוקס).
- ⊙ Netstumbler (למערכת הפעלה Windows). התוכנה תסייע באיתור רכזות באזורך, (Access Point) AP.
- ⊙ Wildpacket airopeek (למערכת הפעלה Windows). התוכנה תסייע באיתור עמדות ברשת שגילית.
- ⊙ וכמובן LANGuard scanner for WLAN (למערכת הפעלה Windows). התוכנה תעניק לך את יכולת הסריקה ברשת.

בפרק הבא מודגם צעד אחר צעד פריצת הצפנת WEP. בכלל הכלים מאוד השתפרו, ופריצה לרשת WEP היא עניין שאורך דקות ספורות בלבד.

לפני שנתקדם, נסקור מספר מושגים בסיסיים:

⊙ MAC Address – הכתובת הפיזית של כרטיס הרשת שלך.

⊙ SSID (Service Set Identifier), מספר שמייצג את שם הרשת האלחוטית.

כצעד ראשון יש לנסות וללכוד את הרשתות שבסביבה. מומלץ להשתמש בכרטיס אלחוטי המצויד באנטנה חזקה שניתן לרכוש באינטרנט, כך תגדיל את שטח הכיסוי. כעת הפעל את תוכנת Netstumbler. התוכנה תוכל לבחור סריקה של SSID וכל מה שיימצא בטווח יופיע לפניך, כולל כתובת MAC של הרכות. כל שנותר כעת הוא להשתמש ב-Sniffer אלחוטי דוגמת Kismet, ומכיוון שאתה יודע את כתובת ה-MAC של הרכות, ניתן לבצע סינון לפי הנדרש מכל ה-Frames שנלכדו.

האקר יכול שלא להסתפק בכך, ובעזרת תוכנה דוגמת ESSID-jack הוא יכול לגרום לעמדה שלך לחשוב שהוא הנתב. לאחר שההאקר יתקין שני כרטיסי רשת, כל התעבורה שלך תעבור למעשה דרכו. הוא גם יכול להשתמש ב-LANguard (השימוש בה יודגם בהמשך) ולראות את השירותים הפעילים והשיתופיים שלך. אם האקר מעוניין לפגוע בכך ולגרום לקריסת המערכת שלך, הוא יתחיל להפציץ את הרשת בעזרת תוכנות שמייצרות מנות (Packets), דוגמת GspooG או LANforge. כתוצאה מכך, הרשת שלך תהפוך לאיטית יותר ויותר עד שתקרוס.

שימוש במערכת מוצפנת דוגמת **WEP** (Wired Equivalent Privacy), לא יעזור בהרבה, כי המערכת מעניקה הגנה למספר שעות בלבד. WEP עובדת אמנם בסיסמה סימטרית חזקה בשם RC4, אולם לתוכנות שמייצרות מנות יש מנגנון שחוזר על עצמו מדי $2^{24}=16M$ מנות. לכן ההאקר יתחבר לרשת שלך ויתחיל ליזום תעבורה, במקביל לשימוש בכלי פריצה דוגמת Airsnorts או Webrack. כדי להתגבר על הבעיה פותח תקן אבטחה בשם **WPA** (Wi-Fi Protected Access), שפותר את בעיות האבטחה של WEP ובין השאר דואג לייצור בתדירות גבוהה של מפתח ההצפנה. הדבר מקשה על ההאקר את הפריצה, מכיוון שהוא מתקשה לחלץ את הקוד בפרק זמן קצר מאוד. עם זאת, במערכת גדולה ייתכן חוסר תיאום בתקנים שיפורטו להלן, והדבר עלול להקל על ההאקר.

בפרק "כלי תקיפה" הבא, תלמד כיצד פורצים בקלות רשתות אלחוטיות עם אבטחה מסוג WEP.

ברמת העיקרון, קח בחשבון שלא כל כרטיס רשת אלחוטי מתאים למטרה זו. היכולת להזריק נתונים לתוך התעבורה האלחוטית תלויה ב-chip set של הכרטיס.

כרטיס רשת אלחוטי מוגדר להאזין לתעבורה שממוענת אליו וממנו. כדי להעביר את הכרטיס למצב של monitoring יש להיעזר בתוכנת AirmoN. כרטיסי Ethernet נקראים במערכות לינוקס eth ולזה מצטרף מספר ההתקן, למשל eth0. כרטיסים אלחוטיים נקראים לעומת זאת wlan.

בעיות אבטחה הקשורות לשכבות 5-7 של מודל השכבות

כידוע, שכבות אלו עוסקות ביישום עצמו. כאן נראה התייחסות לנושאים כגון: פריצת סיסמאות, התקפת שרתים, גניבת מידע וכן בהמשך התייחסות להקשחת שרתים. גם הווירוסים, ה-Spy והסוסים הטרויאנים ידונו כאן.

סיסמאות

סיסמאות הן נקודה חשובה וכואבת. לכאורה דברים השתנו מאז ימי Windows 98 העליזים, אז המערכת אחסנה את הסיסמאות בקבצים עם סיומת `pwd`, אותה היה קל למחוק או לשנות לסיומת אחרת. כך יכלו אנשים להיכנס למערכת ללא סיסמה. לא שבמערכות אחרות המצב כל כך מזהיר:

לינוקס לדוגמה משתמשת ביישום החשבונות והסיסמאות בקבצים `/etc/passwd` ו-`/etc/shadow`. לכאורה זה מוצפן והכל יעיל. אך בפועל אין שום הגנה מקומית, כל משתמש יכול לכבות את המחשב, להעלותו במצב תחזוקה ולשנות את סיסמת המפקח.

נוהל העבודה המפורט בפריצת סיסמת מפקח בלינוקס יצוין בהמשך, אך כאן אציין בקיצור שכל מה שיש לעשות הוא לאתחל את המחשב, ברגע שיופיע מולך ה-`logo` של Lilo הקש על `Ctrl+X`, ואז במסך הקלד `linux single` (יש מערכות בהן תידרש להקליד `linux rescue`). לאחר שיוצגו מספר שורות, תוכל להקליד `passwd` ואת הסיסמה החדשה של המפקח.

לא מדהים? וכל אנשי Linux מודעים לכך.

Windows – נניח שהתקבלת לעבודה בארגון והתברר לך שאינך יודע מהי הסיסמה, או שאחד העובדים בוחן את מנהל הרשת החדש ומשנה את הסיסמה. תוכנת עזר בשם ERD (כיום שונה השם ל-DaRT) מאפשרת לך לבצע אתחול מהתקליטור, ואז דרך התפריטים `Start ← Programs ← Keylock` ולשנות את סיסמת המפקח מבלי לדעת את הסיסמה הקודמת!!

מה המשותף לכל הפריצות שצוינו כאן? בכולן הייתה גישה מקומית לשרת! וזה הלקח, לעולם אל תאפשר גישה מקומית לשרת, הקפד לנעול את חדר השרתים כשאינך נמצא בחדר.

ודא שאין אפשרות להתחבר ב-Terminal Server לבקר `domain`. מיקרוסופט ממליצה בחום להתקין שרתי Terminal על שרתים שאינם בקרי `domain`, בין היתר מכיוון שכדי לאפשר את העבודה אנו מעניקים לעובדים זכות `Log on Locally` ובבקר `domain` ההרשאה הזו גולשת ליתר השרתים (כעיקרון כאשר מגדירים משתמש חדש, הוא יכול לבצע `Logon` לרשת מכל

מחשב מלבד דרך השרתים עצמם. הוא לא יכול לגשת ישירות לשרת ולבצע ישירות Login ממנו. כדי שיוכל לעשות זאת, עליו לקבל הרשאת (Log on Locally).

תוכנות לפריצת סיסמאות

קיימות מספר תוכנות מוכרות לפריצת סיסמאות, לדוגמה:

LC4 ו-NAT (Netbios Auditing Tool) שמתמחות בעיקר בפיצוח דרך הרשת.

John the ripper, Crack-1 ו-Pwdumps2 שמתמחות בפריצה מקומית.

יש תוכנות שמיועדות לשרתים וציוד אחר דוגמת GetPass, שמבצעת פענוח לסיסמאות של נתבי CISCO.

קח בחשבון שסיסמאות רבות פועלות במנגנון hashing algorithm, מנגנון הצפנה מסוג one way דוגמת MD5 או DES. נושא זה הוסבר בפרק הראשון וגם כאן בהמשך, לכן רק אזכיר שהמנגנון מקבל מידע ומציפין אותו באופן בו לא ניתן יהיה להקיש מהמידע המוצפן על תוכן המידע ה"נקי". משתמש מתוחכם יקח סיסמה מוכרת (אולי אפילו את הסיסמה שלו) וינסה לפענח את מנגנון ההצפנה. הוא יריץ את הסיסמה מול האלגוריתם שפיתח או הוריד מהאינטרנט וישווה במקביל את המהירות של פענוח הסיסמה דרך הרשת, זאת כדי לנסות ולהגיע לזמנים שווים שיצביעו על הנוסחה הנכונה.

תוכנה דוגמת NAT מנסה לנצל חולשות מסוימות בפרוטוקול SMB שמשמש לשיתוף קבצים והדפסה. אחרי שתוריד את התוכנה מהאתר www.securityfocus.com/tools, תריץ את הפקודה `ip address nat -u userlist.txt -p passlist.txt` (במקום ip address של השרת אותו אתה עומד לבדוק). בתגובה תנסה המערכת לחלץ את שמות החשבונות והסיסמאות ולהציג אותם בקובץ.

זכור שכולם יודעים היכן מאוחסנות הסיסמאות:

Windows – במחשב שפועל עצמאית או ברשת שיווינית, הסיסמאות מאוחסנות במסד נתונים קטן שנקרא SAM, והוא נמצא ב- `winnt/system32/config`. ברשתות המבוססות על Active Directory, הסיסמאות יאוחסנו בקובץ `ntds.dit`. זכור שכאשר יוצרים דיסקטי הצלה או כלי הצלה, הם לעתים נדרשים להכיל את הסיסמאות, לכן הקפד לשמור עליהם.

Linux – `/etc/passwd` (רשימת החשבונות), `/etc/shadow` (מיקום הסיסמאות המוצפנות) `/etc/security/passwd`. בדוגמה הבאה ניתן לראות סיסמה מוצפנת בקובץ `shadow`.

```
ntp:!!:13156:0:99999:7:::
gdm:!!:13156:0:99999:7:::
user:$1$btdpSDE7$/4iuzKmb6c0n0K6QYFLDX/:13156:0:99999:7:::
named:!!:13164:~::~:
```


אם ההאקר מעריך שבארגון משתמשים בסיסמאות פשוטות, הוא ינסה תחילה להפעיל מפצחים פשוטים שינסו אלפי פעמים לסרוק את מסד הנתונים של הסיסמאות. התקפות אלו קרויות Dictionary Attacks (ניתן להוריד תוכנות כאלו מאתרים, דוגמת: www.outpost9.com - packetstormsecurity.nl).

אם הוא יחשוב שהסיסמאות מורכבות יותר, הוא יעבור לסוג שנקרא Brute-Force Attacks. התקפה מסוג זה יכולה לפרוץ כל סיסמה והשאלה היא רק של זמן. בשיטה זו ינוסו מספר רב של שילובים שיכללו אותיות, ספרות ותווים. לכאורה תהליך הפריצה ארוך, אך קח בחשבון שרוב המשתמשים בוחרים מטעמי נוחות בסיסמאות קלות וקצרות. לפיכך הלקחים הם:

- ⊙ לכפות על המשתמשים שימוש בסיסמה ארוכה (המהדרין יבקשו 16 תווים, נסה לכפות לא פחות מ-15 למרות שברוב המקומות מבקשים 8).
- ⊙ חייב שימוש בסיסמה מורכבת שתכלול אותיות קטנות, אותיות גדולות, ספרות (אפשר לשלב גם תווים מיוחדים, דוגמת @).
- ⊙ יש לשנות סיסמה מעת לעת, לכל המאוחר לאחר חודש. כך ההאקר יאלץ לפצח מחדש את הסיסמה.
- ⊙ הגדר חסימת חשבון לאחר שלושה ניסיונות שגויים של הקלדת סיסמה.
- ⊙ היזהר משימוש באפשרות run as. חשוב על המקרה שבו משתמש כלשהו רוצה להריץ משהו מהשרת, או שיש בעיה כלשהי ואתה מעוניין לפתור אותה במהירות. במצבים כאלה, מנהלי רשת נוטים להשתמש באפשרות זו כדי להריץ תוכנות המחייבות הרשאת מפקח מהעמדה של המשתמש. ייתכן בסבירות לא נמוכה, שהמשתמש התקין תוכנה שלוכדת את כל ההקלדות ואז הוא יכול לזהות את סיסמת המפקח. במקרה זה הוא יוכל להעניק לחשבון שלו הרשאות מפקח ומעתה ואילך יהיה לך, כמפקח, שותף סמוי. בדוגמה הבאה ראה את התוכנה Perfect Keylogger, שמבצעת מעקב אחר כל ההקלדות במחשב ואף מאפשרת, לשם הנוחות, לבחור ולצפות בהקלדות לפי תאריך. בדוגמה הבאה המשתמש הפעיל תוכנה שלוכדת את ההקלדות, וכך ניתן לראות בבירור שהמפקח נכנס להגדרת VLAN1 ברכוזת ושינה הגדרות. כל הקלדה נרשמת. ההאקר יכול לפעול בדרך דומה כאשר הוא מתחזה למשתמש מורשה, או לאחר שפרץ למערכת.

איסוף מידע ופגיעה ברמת רשת

סעיף זה יתמקד בניסיונות זיהוי שירותים מרוחקים, ואפשרויות הפגיעה בהם.

כפי שצויין, החלק הראשון בעבודת ההאקר הוא לימוד המערכת שלך. פעולה זו יכולה להימשך ימים ושבועות, ובמהלכה ייאסף מידע רב על הארגון, כגון: איזה שירותים אתה מפעיל, איזה שרתים קיימים בארגון, מהן גרסאות השרתים, מהו ה- Service pack שהותקן.

כדי לבצע זאת, על ההאקר לאסוף מידע. אחת הדרכים הפשוטות היא לבצע סוגים שונים של סריקות על פורטים, למשל כדי לראות לפי התשובות שיתקבלו אילו שירותים קיימים. אם לדוגמה יש תשובה בפורט 80, משמעות הדבר שיש לך שרת Web. מכאן ינסה ההאקר לגלות פרצות בשרת ודרך Exploit לחדור אליו.

כיום תוכנות Firewall מזהות ומתריעות על פעולות סריקה שמבוצעות. בפרק 4 יש דוגמה המראה כיצד חוסמים סריקה של פורטים רבים מדי. האקרים יודעים שניסיונות אלה מתגלים, ולכן הם תוקפים ממחשבים שונים. האקרים גם יודעים שלמנהל רשת ממוצע אין זמן להתמודד עימם ולקרוא את הדוחות שמפיק עבורו ה-Firewall. לעתים מנהל הרשת מתקין את ה-Firewall, אך בדרך כלל חברה שעוסקת בתחום מבצעת זאת עבורו, והוא מסתפק בידיעה שיש שירות של Firewall. כך קורה שאיש לא מתייחס לכך שמבוצעת סריקה חיצונית על הארגון. זכור שהאקר מתוחכם יגרום לכך שהמחשב שלך "יחשוב" שהסריקה מבוצעת בכלל ממחשב אחר, וכך לא תהיה תגובה למניעת הפעולה או חסימתה.

בין הכלים שנזכיר בפרק יהיו NMAP, Superscan, Netcat, LANguard, Nessus. כולם כלים שניתן להוריד מהאינטרנט, והם עוסקים בזיהוי ואיתור של שירותים.

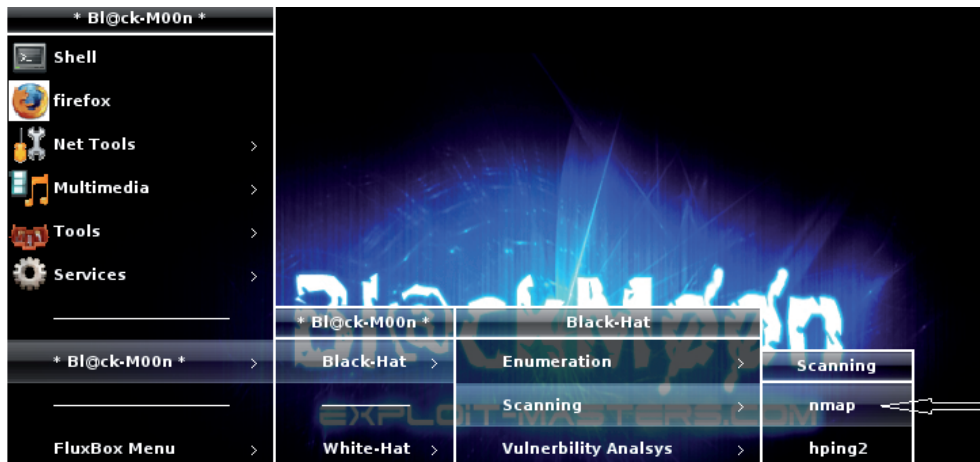
כלי איתור של עמדות ושירותים

לפני קריאת הסעיף, מומלץ לקרוא שוב על פורטים בפרק הראשון.

NMAP – כלי זה (ויש גם אחרים) יסייע להאקר באיתור עמדות פעילות. היעזר במתג `-sP` כדי שיבצע סריקה של `ping`. הוסף, אם אתה מעוניין בכך, את המתג `-n` כדי שימנע את חילוף שמות המחשבים. כדאי גם להוסיף את המתג `T 4` כדי לשפר מהירות. לדוגמה, אם תקליד את הפקודה `192.168.2.1-254 -n -sP -T 4 nmap`, פעולת הסריקה תבוצע כולה על רשת `192.168.2.0`.

המתג `-sS` מאוד שימושי אצל ההאקרים. אחת מהיכולות החשובות של האקר היא לסרוק את המערכת מבלי שמערכת ההתרעה שנקראת IDS תתריע על כך. אם תוכנה שולחת `ping` ללא הפסקה לכל הפורטים, כדי לראות אם יש תגובה, מערכת ההתרעה תזהה ותתעד זאת בקבצי `log`. המתג `-sS` נקרא `Stealth Port Scan`. בזכות מתג זה NMAP תשלח דגל SYN ותמתין

לתגובה. אם יש שירות פעיל באותו פורט, תוחזר תשובה SYN/ACK ואז NMAP תשלח דגל RST והקשר נסגר. כך לא נשארו קשרי TCP פתוחים לשווא, הכל זרם לפי הפרוטוקול וההאקר גילה שהפורט פעיל מבלי שה-IDS ידווח על כך.



כמות המתגים האפשריים בכלי זה היא עצומה. ניתן לבצע לרדוגמה סריקה, שבה המחשב שנסרק סבור היה שמחשב אחר סורק אותו.

```
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--log-errors: Log errors/warnings to the normal-format output file
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enables OS detection and Version detection, Script scanning and Traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sP 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -PN -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root:/Security/Black-Hat/Scanning/nmap-5.21#
```

את הכלי NMAP ניתן להוריד בקלות מהאינטרנט, הן ל-Windows והן ללינוקס. **Superscan** – כלי פופולרי ונוח לשימוש שמאפשר סריקת טווח פורטים ועמדות. ההבדל העיקרי בינו לבין הקודם הוא בהיותו גרפי.

כלים לפגיעה בשירותים

לאחר שהאקר גילה את השרתים הקיימים, הוא ינסה לפגוע בהם. מכיוון שהוא יודע את כתובת ה-IP של נותני השירותים (נותן השירותים הוא כמוכן שרת), ויודע אילו פורטים פתוחים, הוא ינסה להתחיל עם פורטים שפועלים ב-TCP, תוך ניצול העובדה שבפרוטוקול זה יש מנגנון של בקרה ושניתן לשבש אותו. לאחר החיבור הראשוני לשרת, הוא יוכל לבצע מגוון פעולות, דוגמת שליחת הודעות סיום ובכך להפיל התקשרויות, או לפנות פעמים רבות לאותו שרת ולגרום להתקפת SYN Attack שכבר צוינה.

⊙ **Nmapwin** – תוכנה נוחה ושימושית. מעניקה לך אפשרויות התקפה רבות מתוך התפריט המוצג לפניך. מומלץ להוריד את התוכנה ולנסות לבדוק כיצד מערכת ההתרעה שלך מתמודדת מולה. זוהי דרך מצוינת לבחון את ה-Firewall ואת ה-IDS (נושא IDS ושאר הכלים לזיהוי חריגות ברשת יידונו בפרק 5). קח בחשבון שהאקר מתוחכם יבצע את הבדיקה בכל פעם ממחשב אחר וכך יגרום לתוכנת IDS לספק מידע שונה בכל פעם.

⊙ **Get if** – אם בסריקת הפורטים התגלתה תשובה מפורטת 161, משמעות הדבר שאותה עמדה פועלת בפרוטוקול SNMP. כעת ניתן להוריד מהאינטרנט כל תוכנה שקוראת מידע אודות SNMP דוגמת Getif, SolarWinds, ובהנחה שמוגדרת קבוצת ברירת המחדל public, עליך רק לציין את שם הקבוצה והמידע ייאסף אליך. אל תקל בכך ראש. דרך SNMP ניתן לאסוף את המידע המאוחסן בנתב, לדוגמה: טבלאות ניתוב, הגדרות, כתובות ועוד. לפיכך מומלץ להוריד את התמיכה בשירות מכל העמדות שאינן עושות בכך שימוש (בשרתי Windows 2003 זה סגור כברירת מחדל). היכן שיש צורך ב-SNMP, שנה את שם קבוצת ברירת המחדל. מומלץ אף לשדרג את גרסת SNMP. לסיום, בהגדרות ה-Firewall שלך, ודא שלא ניתן לגשת בפורט 161 אל הרשת הממוקמת ב-DMZ (נושא DMZ נידון במספר מקומות בספר זה, כאן אציין בקיצור שזוהי רשת קטנה הנמצאת בין הרשת הפנימית בארגון לבין הרשת החיצונית). ניתן גם להיעזר בתוכנה snmpenum למטרות איסוף מידע תוך ניצול העובדה שמשמשים ב-SNMP.

⊙ שימוש ב-Telnet כדי להיכנס לשרתים ולאסוף מידע. את הדוגמה הבאה בצע צעד אחר צעד על שרת הדואר שלך, כדי לראות שהיא עובדת מבלי לפגוע באחרים. עבור לשורת הפקודה cmd והקלד telnet. מכיוון שאתה בודק על שרת הדואר שלך, הקלד set local_echo (לעתים יש להקליד set localecho). כעת גש לפורט המתאים: open localhost 110 (פורט זה משמש למטרת pop3 שרוב המשתמשים מקבלים דרכו דוא"ל). במציאות מאחדים את השורות וכותבים telnet ip-address port, לדוגמה: (telnet 192.168.5.1 110). כעת עליך להזדהות. הקלד את המילה user

הקדשת תשומת לב ל-Processes

בסעיפים קודמים הוזכר נושא תוכנות Spy שמושגות במחשב ללא ידיעת המותקף, ואף הודגמה תוכנה שמבצעת זאת. רוב תוכנות ה-Spy אינן גאוניות, ובדרך כלל הן יופיעו לפניך ברשימת ה-processes אליה תגיע דרך הקשה על Alt+Ctrl+Del. הבעיה היא שכאן רשימת ה-processes שתקבל ארוכה מרשימת התוכנות שאתה רואה בכרטיסייה Application, מה גם שאינך יכול לדעת ממסך זה איזו תוכנית הפעילה process מסוים. ניתן אמנם לקבל מידע חלקי על ידי הרצת הפקודה msconfig ולראות את שמות התוכנות שמופעלות אוטומטית ואת שם ה-process, כמו בדוגמה הבאה:

Startup Item	Command	Location
<input checked="" type="checkbox"/> ShowBehind	D:\WINDOWS\sbnet>ShowBehind.exe	HKLM\SOFTWARE\Mic
<input checked="" type="checkbox"/> VPtray	D:\PROGRA~1\SYMAN~1\VPtray.exe	HKLM\SOFTWARE\Mic
<input checked="" type="checkbox"/> winampa	D:\Program Files\Winamp\winampa.exe	HKLM\SOFTWARE\Mic
<input checked="" type="checkbox"/> ctfmon	D:\WINDOWS\System32\ctfmon.exe	HKCU\SOFTWARE\Mic
<input checked="" type="checkbox"/> msmgs	"D:\Program Files\Messenger\msmsgs.exe" /background	HKCU\SOFTWARE\Mic
<input checked="" type="checkbox"/> Microsoft Office	D:\PROGRA~1\MICROS~2\Office\OSA9.EXE -b -l	Common Startup

אבל זו רשימה חלקית. כל מי שיבדוק במחשבו דרך Task Manager, יראה שהרשימה האמיתית ארוכה בהרבה.

Image Name	User Name	CPU	Mem Usage
svchost.exe	SYSTEM	00	268 K
taskmgr.exe	doron	02	4,036 K
WINWORD.EXE	doron	98	27,264 K
wuauclt.exe	doron	00	192 K
wdfmgr.exe	LOCAL SERVICE	00	32 K
mspaint.exe	doron	00	14,168 K
Rtvsan.exe	SYSTEM	00	2,300 K
msmsgs.exe	doron	00	120 K
ctfmon.exe	doron	00	316 K
winampa.exe	doron	00	180 K
VPtray.exe	doron	00	420 K
ShowBehind.exe	doron	00	528 K
pds.exe	SYSTEM	00	124 K
inetinfo.exe	SYSTEM	00	464 K
DefWatch.exe	SYSTEM	00	40 K
alg.exe	LOCAL SERVICE	00	72 K
EXPLORER.EXE	doron	00	5,680 K

Select Columns	
Select the columns that will appear on the Process page of the Task Manager.	
<input checked="" type="checkbox"/> Image Name	<input type="checkbox"/> Page Faults Delta
<input type="checkbox"/> PID (Process Identifier)	<input type="checkbox"/> Virtual Memory Size
<input checked="" type="checkbox"/> CPU Usage	<input type="checkbox"/> Paged Pool
<input type="checkbox"/> CPU Time	<input type="checkbox"/> Non-paged Pool
<input checked="" type="checkbox"/> Memory Usage	<input type="checkbox"/> Base Priority
<input type="checkbox"/> Memory Usage Delta	<input type="checkbox"/> Handle Count
<input type="checkbox"/> Peak Memory Usage	<input type="checkbox"/> Thread Count
<input type="checkbox"/> Page Faults	<input type="checkbox"/> GDI Objects
<input type="checkbox"/> USER Objects	<input type="checkbox"/> I/O Writes
<input type="checkbox"/> I/O Reads	<input type="checkbox"/> I/O Write Bytes
<input type="checkbox"/> I/O Read Bytes	<input type="checkbox"/> I/O Other
<input type="checkbox"/> Session ID	<input type="checkbox"/> I/O Other Bytes
<input checked="" type="checkbox"/> User Name	

כפי שאתה רואה, למרות שניתן דרך View – Select Columns להגיע למסך שנראה למעלה מימין ולהוסיף עמודות עם מידע רב, עדיין רב הנסתר על הגלוי. זו דרישה לגיטימית, לדעת איזה יישום הפעיל את ה-process במחשב שלי. קיימות תוכנות באינטרנט, דוגמת Security Task Manager מהאתר www.neuber.com/taskmanager/process, בהן תמצא פירוט על processes רבים וכן תוכנה ללא תשלום שתבצע סריקה עבורך.

You find information and user opinions about common Windows processes in our Process and Task list.

System Processes

[alg.exe](#) [csrss.exe](#) [ctfmon.exe](#) [dllhost.exe](#) [explorer.exe](#) [internat.exe](#) [kernel32.dll](#) [lsass.exe](#) [mdm.exe](#) [msmsgs.exe](#) [mstask.exe](#) [regsvc.exe](#) [rundll32.exe](#) [services.exe](#) [smss.exe](#) [spoolsv.exe](#) [svchost.exe](#) [system](#) [winlogon.exe](#) [winmgmt.exe](#) [wisptis.exe](#) [wmieex.exe](#) [wmprievs.exe](#) [wscntfy.exe](#) [wuauclt.exe](#)

Application Processes

[ati2evxx.exe](#) [avguard.exe](#) [ccapp.exe](#) [ccevmtgr.exe](#) [ccsetmgr.exe](#) [ctagent.dll](#) [defwatch.exe](#) [dit.exe](#) [em_exec.exe](#) [ezsp_px.exe](#) [gearsec.exe](#) [hkcmd.exe](#) [htpatch.exe](#) [iexplore.exe](#) [jusched.exe](#) [mcshield.exe](#) [mcvseecn.exe](#) [mspmbspv.exe](#) [navapsvc.exe](#) [navshext.dll](#) [nprotect.exe](#) [nsvsc32.exe](#) [nwiz.exe](#) [pctspk.exe](#) [point32.exe](#) [qttask.exe](#) [smc.exe](#) [taskman.exe](#) [vsmon.exe](#) [webscanx.exe](#)

Malware Processes

[2_0_1browserhelper2.dll](#) [alchem.exe](#) [belt.exe](#) [bridge.dll](#) [cmesys.exe](#) [gmt.exe](#) [istsvc.exe](#) [msbb.exe](#) [mslaugh.exe](#) [mxtarget.dll](#) [newdot~2.dll](#) [optimize.exe](#) [save.exe](#) [sp.exe](#) [twaintec.dll](#) [updmgr.exe](#) [winnet.dll](#) [wuamgrd.exe](#) [wupdater.exe](#)

Security Task
An enhanced process all the standard information, unique security risk analysis of hidden file stealth, browser surveillance, entry,...

Click image to see

Free download

Buy now

לאחר ההתקנה, הרץ את התוכנית ותקבל את הפלט הבא. שים לב להבדל בהתייחסות של שתי התוכנות אל התוכנה Paint שהרצתי במחשב.

Process Name	Private Bytes	Working Set	Private Bytes	Working Set	Path	Company Name	Process Name	Process Name
Symantec AntiVirus Client	44	0%	16.2 MB	C:\Program Files\Symantec_Client\Hrtvscan.exe	Program	VPIPLINK		
SoundMAX service age...	42	0%	1.7 MB	C:\Program Files\Analog Device\SMAGENT.exe	Program			
Symantec AntiVirus Client	27	0%	1.4 MB	C:\Program Files\Symantec_Client\DefWatch.exe	Program	Virus Definition Daemon		
hkcmd Module	24	0%	0.3 MB	C:\WINDOWS\System32\hkcmd.exe	Program	HK\WndName		
LC5	24	0%	1.3 MB	C:\Program Files\@stake\LC5\lc5.exe	Program	@stake LC5 - [Untitled		
SoundMAX System Tray		0%	0.3 MB	C:\Program Files\Analog Device\SMTRAY.exe	Taskicon	SoundMAX Tray, So		
WinZip Executable		0%	0.3 MB	C:\Program Files\WinZip\WZQKPKICK.EXE	Taskicon	About WinZip Quick		
Cain & Abel v2.68		0%	1.7 MB	C:\Program Files\Cain\Cain.exe	Program	Cain - Password Rec		
Virtual PC		1%	7.5 MB	C:\Program Files\Microsoft Virtual PC\Virtual PC.exe	Program	2276C-DEN-SRV1 - I		
SolarWinds 2002 Profes...		0%	1.3 MB	C:\Program Files\SolarWinds\SolarWinds-Toolbar.exe	Taskicon	SolarWinds Network		
Symantec AntiVirus Client		0%	0.5 MB	C:\Program Files\Symantec_Client\WPTray.exe	Taskicon	Symantec AntiVirus C		
Microsoft Office Professi...		0%	1.1 MB	C:\Program Files\Microsoft Office\POWERPNT.EXE	Program	Microsoft Office Pow		
igfxTray Module		0%	0.2 MB	C:\WINDOWS\System32\igfxtray.exe	Taskicon	igfxtray\Window, Intel		
Security Task Manager		2%	3.1 MB	C:\Program Files\Security Task Manager\Taskman.exe	Program	Security Task Manag		
Internet Explorer		0%	2.7 MB	C:\Program Files\Internet Explorer\iexplore.exe	Program	Security Task Manag		
Windows Explorer		0%	12.7 MB	C:\WINDOWS\Explorer.EXE	Program	Program Manager, V		
Paint		0%	0.7 MB	C:\WINDOWS\system32\mspaint.exe	Program	task1.bmp - Paint		

Image Name	User Name	CPU	Mem Usage
svchost.exe	SYSTEM	00	4,696 K
mspaint.exe	jbt	00	716 K

הרשימה שלעיל חלקית בלבד. כאשר תבחר בחלק העליון של המסך באפשרות Windows processes, תקבל רשימה מפורטת יותר, הכוללת processes שמערכת ההפעלה מפעילה בעצמה. בשלב זה רוב התוכנות שמנסות להתחבא ימצאו, ובחלק התחתון של המסך תוכל לראות בפירוט מה עושה אותו process.

וירוסים ותוכנות ריגול (Spy)

מטרת הסעיפים הבאים היא לפרט בפני הקורא את נושא הווירוסים ותוכנות הריגול (Spy) כדי להשלים את התמונה מבחינת התקפות על מחשבים.

נתחיל מסקירה קצרה של המושגים ובהמשך נעבור לפירוט מקיף:

וירוס – תוכנה שנקשרת לתוכנה אחרת או לקובץ, ופוגעת במחשב וברשת.

וירוס מסוג rabbit – תוכנה שמשכפלת את עצמה בדיסק הקשיח ובזיכרון וגורמת להאטה ולקריסה.

תולעת, Worm – תוכנה שמשכפלת את עצמה גם דרך הרשת. לא זקוקה להיצמד לתוכנה אחרת כמו וירוס.

סוס טרויאני – תוכנה שמתחזה לתוכנה אחרת. אתה מפעיל תוכנה מסוימת ובפועל מפעיל תוכנה אחרת. בהמשך אביא שתי דוגמאות לכך.

דלת אחורית, Back door – סוסים טרויאנים, פותחים לעתים דלת דרכה האקר יכול להיכנס למחשב שלכם.

חדירה, Intrusion – חדירה למחשב יעד. זאת משיגים לדוגמה בעזרת דלת אחורית, Exploit שמודגם בספר ועוד.

מהם וירוסים?

וירוס הוא תוכנת מחשב שאופן כתיבתה רגיל, אך מטרתה לגרום נזק. כאשר הווירוס כבר חודר לזיכרון המחשב, הוא יפעל על פי הסוג שאליו הוא משתייך. ניתן להבחין במספר סוגי וירוסים:

1) וירוסים שנדבקים ל- **Boot sector** (רשומת האתחול).

בעת הפעלת המחשב ניגש ה-BIOS אל הדיסק ומתחיל התהליך המוכר של טעינת DBR, MBR וכל גזרת האתחול. בדרך זו מובטח לוירוס שבכל הפעלה של המחשב הוא יוטען לזיכרון. מאותו רגע אנו בני ערובה של הווירוס. כל פנייה להתקן עוברת דרך ה-BIOS ומכיוון שהוא נשלט כעת על ידי הווירוס, הרי שהוא יכול לבצע את זממו מבלי שנהיה מודעים לכך. לדוגמה, וירוס מסוג rabbit ינסה לשכפל את עצמו למחשבים אחרים. אופן העבודה של וירוסים מסוג זה לא אחיד, כמובן. חלקם מחליפים לחלוטין את פקודות האתחול הראשוניות וחלקם שותלים הוראות דילוג למקום בו התנחלו בזיכרון המחשב. וירוסים מסוג זה מחפשים לרוב בזיכרון את BPB (Block Parameter BIOS) שמכיל נתונים רבים וחשובים על הדיסק. בעת ההפעלה

3

כלי תקיפה מתקדמים

סקירת כלי תקיפה - BlackMoon 2.0

הפצת BlackMoon היא הפצת אבטחה מבוססת לינוקס, שמטרתה לעזור למקצועני אבטחת מידע לערוך מבדקי אבטחה. בפרק מתוארת גרסה 2.0. ניתן להורידה מהאתר או את גרסה 3 החדשה יותר. היכנס לאתר כדי להוריד את הגרסה העדכנית ביותר.

הערה!



בסוף הפרק תמצא סקירה קצרה על לינוקס. למידע רב יותר פנה לספר "מדריך ושנתות טכנאי PC ולמנהלי רשת".

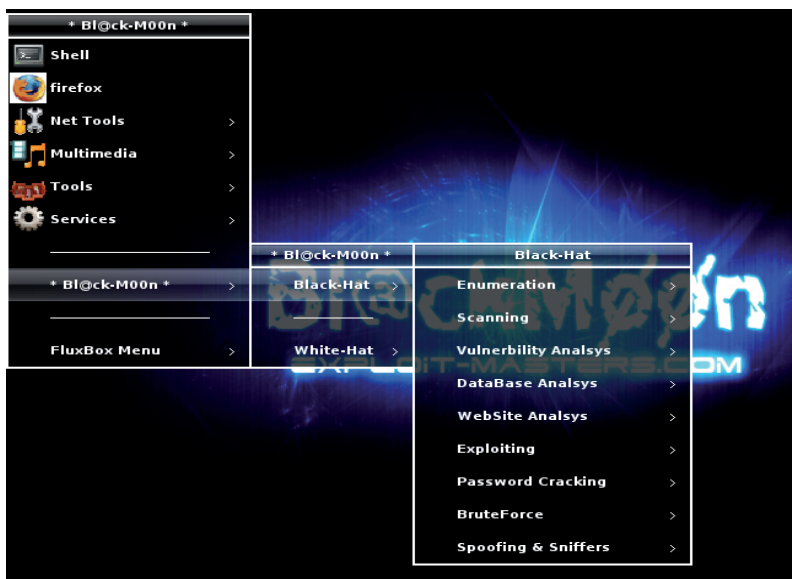
תכונות המערכת:

- (1) מיועדת למטרות אלו ולכן אופן העבודה נוח ומקצועי.
- (2) ניתן להריץ אותה מדיסק או כונן שליף, ללא צורך בהתקנה או הגדרה. אפשר גם להפעיל אותה באופן וירטואלי, דרך Hyper-V, Vmware ועוד.
- (3) מערכת BlackMoon מיועדת לקהל רחב מאוד, החל ממקצועני אבטחת מידע ועד אנשים עם ידע מועט בתחום.
- (4) התוכנה היא ללא תשלום וניתנת להורדה מהאתר www.exploit-masters.com. בכניסה לאתר יש לבחור **BlackHat** או **WhiteHat** ודרך לשונית Products לבחור בהורדת המערכת.

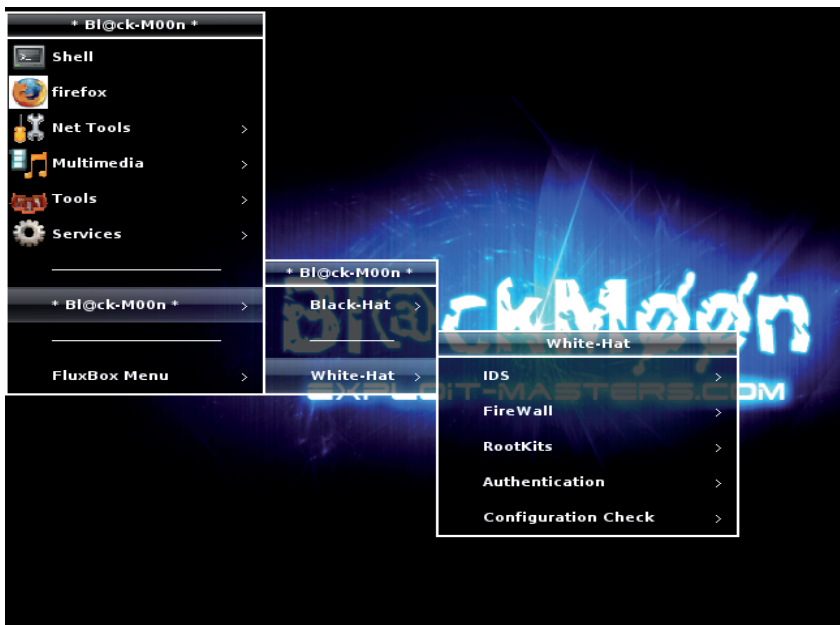


הקו המנחה הן באתר והן במוצרים, הם החלוקה לשני הכיוונים:

BlackHat - האקרים או אנשי אבטחת מידע שיש ברשותם ידע רב ויכולים בעזרת המערכת לתקוף מערכות מחשוב. בחירה בקטגוריה זו, תוביל לבחירה בתפריטי משנה עבור כלי תקיפה מתקדמים, כמפורט בהמשך.



WhiteHat - אנשי סיסטם או מנהלי רשתות שיכולים בעזרת המערכת ללמוד ולהעריך את אבטחת המערכות שלהם. מינוח נפוץ נוסף הוא **Ethical Hacker**, כלומר האקר שעושה שימוש חיובי בידע שלנו. בחירה בקטגוריה זו, תוביל לתפריטי משנה של תוכנות אבטחה.



פירוט הכלים שנמצאים בגרסה 2, בחלוקה לקטגוריות:

BlackHat

- ⊙ Enumeration
- ⊙ Scanning
- ⊙ Vulnerability analysys
- ⊙ Database analysys
- ⊙ Website analysys
- ⊙ Exploiting
- ⊙ Password Cracking
- ⊙ Bruteforce
- ⊙ Spoofing & Sniffers

WhiteHat

- ⊙ IDS
- ⊙ FireWall
- ⊙ Rootkits
- ⊙ Authentication
- ⊙ Configuration Check