דו"ח מעבדה- תרחיש מס' 1

# פרטים:

מגיש: דביר ברזילי

תאריך:

שם התרחיש: Apachi shut down

# תהליך ההתקפה:

התוקף עשה סריקת פורטים וניחוש סיסמאות לשרת Apachi1 והתחבר אליו. כתוצאה מכך הוא העביר לתוך השרת וירוס שמפיל את השרת כל דקה, ושולח לעצמו את הקבצים passwd ו-shadow.

# תהליך הזיהוי:

זיהינו בArcSingt שכתובת IP חיצונית 199.203.100.178 מבצעת סריקת פורטים על המחשב Apachi1 ([Fox](http://www.Fox)news) בשעה 13:16 ומייד אחרי זה Password guessing בשעה 13:18. מייד בדקה זו ראינו בלוגים שהוא הצליח להתחבר דרך שירות SSH ובשרת הZenuse הופיע לנו "IP service http is down" בשרת Apachi1.

בשעה 13:11 התחילה מערכה נוספת שבה כתובת IP 199.203.100.30 ביצעה Password guessing לשרת Apachi3. לאחר מכן ראינו בקבצי הלוגים בשרת זה שהפורץ הצליח להתחבר לשרת דרך שירות SSH.

בשעה 13:19 זיהינו בArcSingt שהשרת c מנסה ליצור תקשורת בפורט 80 עם הפורץ (199.203.100.194) .

בנוסף ראינו בלוגים של השרת שרצות פקודות מסויימות כל דקה.

# תהליך הגנה:

כשזיהינו מי התוקפים ומה היעד שלהם ראשית כל חוקקנו חוקים חדשים בFireWall שיחסמו כל תעבורה נכנסת ויוצאת בין הרשת שלנו לפורצים. בנוסף שינינו את הסיסמה לשרת כדי למנוע נסיון חדירה נוסף דרך כתובת שונה. ניסינו להרים חזרה את השרת אך הוא נפל כל פעם מחדש. הבנו שכנראה מדובר בנוזקה שמפילה את השרת באופן אוטומטי. משם התחלנו לחפש בתוך השרת Apachi1 אחר שינויים שנעשו בעקבות הפריצה ונסיון להבין מה הנוזקה שגורמת לנפילת השרת. זיהינו ב-CRON (מתזמן תהליכים בלינוקס) שיש קובץ שרץ כל דקה מחדש עם שתי פקודות, ואחת מהן אחראית על נפילת השרת. הפקודה השנייה אחראית על הרצת קובץ נוסף בשם bd\_bash שגם אחראי על הרצת קובץ פייתון. זיהינו שמטרת התוקף בקבצים אלו הייתה לגנוב את קבצי ה- passwd ו- shadow. בגניבת קבצים אלו המשתמש השיג את דרך הצפנת הססמאות של הארגון, וע"י כך יכול לפענח את כל הססמאות בארגון.

# תהליך הגנה מונעת:

שינוי סיסמאות בארגון. אילולא סיסמאות כאלו פשוטות (פריצה לאחר ניחוש חמישי!) הפורץ לא היה מצליח להחדיר ולגנוב קבצים ממחשבי הארגון. בנוסף כדאי לסגור את פורט 20 לפחות לתקשורת חיצונית, ובאופן כללי להיות בביקורת עליו ולאפשר גישות באופן נקודתי בעת הצורך. הגנה נוספת אפשרית היא לא ליצור הרשאות גישה (read only למי שאינו root וכדומה), למרות שבמקרה שלנו הפורץ הגיע להרשאת root.

# הפרצות באבטחת הארגון

סיסמאות פשוטות מידי. הרשאות לשינוי כתיבה וקריאה לכל אדם.

# כלים שפיתחנו

# אופן עבודת הצוות

הייתה עמדת "מחוקק" שדאגה לחסום את התוקפים ב-Firewall לאחר שזיהינו אותם. באופן כללי היינו כל הזמן בביקורת על הכלים השונים ודאגנו לפקח ולאתר ארועים חשודים. לאחר שנטרלנו את התוקף וחסמנו אותו, נרתמנו לאיתור הבעייה שגורמת לשרת ליפול ע"מ לטפל בנזק שנגרם. החיפוש לקח זמן רב יחסית ודרש גם קריאה ולמידה של דברים חדשים באינטרנט שלא ידענו את משמעותם קודם לכן.

# חוסרים/קשיים

קושי בזיהוי מטרת הפורצים ומה בדיוק הם ניסו לעשות בתוך השרתים. בנוסף אחרי שהשירות HTTP בשרת Apachi1 נפל התקשנו להעלות אותו מחדש, אנו חשדנו שיש ווירוס שמפיל את השרת כל פעם מחדש וזה לא אירוע חד פעמי.

קושי נוסף היה שהפורץ עשה "רעש" וניסה לפרוץ גם לשרת Apachi3.