Layer 2 Defence - Port Security

מאת רון הרניק (The Ping Factory)

הקדמה למאמר

מאמר זה נכתב ע"י רון הרניק, מרצה במכללת IITC להסמכות CCNA, CCNA Security, CCNP, JNCIA ובמקביל מפעיל את הבלוג "The Ping Factory", בלוג מקצועי / לימודי המתעסק בתקשורת נתונים, המיועד גם למתחילים את דרכם בתחום ולמקצוענים כאחד. המאמר הנ"ל נכתב כפוסט במסגרת הבלוג.

הקדמה

אנשים נוטים להתעלם בדרך כלל מאבטחה ב-Layer 2. ניתן לראות שימוש בפתרונות אבטחה מתקדמים, בין אם הם של חברות כגון Cisco, Checkpoint, Fortinet, תוך כדי הזנחה של הרמה הנמוכה יותר, הפשוטה יותר של אבטחה.

כאשר אני מדבר על אבטחת רשת, איני מדבר על מערכות Firewall או IPS מתקדמות, וגם לא על הגנה ספציפית מפני מתקפות האקינג. מדובר על קו ההגנה הראשון מפני האנשים המסוכנים ביותר לרשת הארגון שלכם. אתם (בתור אנשי התקשורת של הארגון).

אנחנו, אלו שרוצים להרחיב את הידע שלנו בנושא תקשורת נתונים, שלומדים ל-CCNA ול-CCNP ולהסמכות אחרות - מהווים סכנה גדולה יותר לרשת מאשר כל איום חיצוני. לפני כמה חודשים, תלמיד שלי התקשר אלי בבהלה ואמר לי שהוא מצא מתג (Switch) ישן במעדה בארגון שלו, והוא חשב לעצמו "למה לא נחבר אותו? נראה איך הוא מגיב? מה אפשר ללמוד?", כל מה שהוא רצה זה רק קצת לתרגל את מה שהוא למד. התלמיד הלא-מודע חיבר את המתג לרשת הארגון ולאחר כמה שניות זיהה עצירה כמעט מוחלטת של תעבורה.

מה אנו יכולים ללמוד מן המקרה הזה? דבר ראשון אנחנו יכולים לזהות כשל רציני במדיניות האבטחה הפנימית של הארגון, כל ה-Firewalls שבעולם לא יצילו אותך מפני תלמידי CCNA ו-CCNP. דבר שני, אנחנו יכולים לזהות תכנון לקוי של עץ ה-Spanning Tree של הארגון. מה שללא ספק קרה, זה שהמתג הישן הכריז על עצמו כ-Root Bridge במערכת STP, ולאחר מכן כל הרשת החלה להתכנס לכיוונו. מצב זה

גורם ללינקים מהותיים בתשתית להיחסם בעוד שהנתיבים המובילים אל המתג החדש (הישן) שחובר לרשת נפתחים.

אם אתם עוד לא בקיאים ב-Spanning Tree ולא בדיוק הבנתם על מה אני מדבר זה בסדר (תוכלו לקרוא על כך בפסקה בצד), המטרה הייתה רק להדגים את הצורה שבה התעלמות מהגנות ל-L2 פנימיות יכולה להיות מסוכנת לארגון. אז אם חיבור מתג ישן למערכת הוא דבר מסוכן אחד שיכול לקרות למערכת שלנו, מה עוד אנחנו יכולים למנוע ב-Layer 2?

STP על קצה המזלג

Spanning Tree Protocol הינו פרוטוקול למניעת לולאות והנדסת תעבורה על תשתיות Ethernet.

באמצעות STP המתגים בארגון מתקשרים זה עם זה ובונים היררכיה מסוימת הנקראת "עץ".

אחד מהמתגים נבחר להיות ראש העץ (Root Bridge), ועל כל שאר המתגים במערכת למצוא את הנתיב הטוב ביותר בכדי להגיע לראש העץ. לאחר שכל המתגים מצאו את הדרך הטובה ביותר בכדי להגיע לראש העץ, כל הנתיבים המשניים נחסמים.

מצב זה משאיר רק נתיב אחד פעיל ברשת בין קצה לקצה, ובכך מונע את האפשרות ללולאות. בכדי להגיע ליעילות מקסימלית ולביצועים טובים ברשת, יש לתכנן את העץ בקפידה.

אם משאירים את STP ללא הגדרות, הוא יבחר במתג הישן ביותר (כתובת ה-MAC הנמוכה ביותר) כראש העץ.

אמנם לזה אין לי סיפור לספר לכם, אבל אנחנו יכולים להשתמש במתגים שלנו בשביל סינון גישה על בסיס כתובות MAC. באופן מאוד פשוט, אנו יכולים להגדיר אילו כתובות פיזיות מורשות לעבור את המתג ואילו לא. למשל, יכול להיות שנחליט שבמידה ועובד מנתק את המחשב הארגוני שלו ומחבר את המחשב הנייד לכבל הרשת במקום, התנועה המגיעה ממנו תחסם. האם ניתן לעקוף מנגנון כזה? לזייף כתובות MAC? כמובן, אבל כמו שאמרתי, הסכנות האלו הם לא ממשתמשים זדוניים - אלא משתמשים לא מודעים.

במאמר זה ובמאמרים הבאים נדבר על כמה מנגנוני הגנה ב-Layer 2 שניתן ליישם על מתגים. אנו נשתמש במתגי Cisco לדוגמה.

Port-Security

Port-Security הוא מנגנון המאפשר לנו לסנן גישה על בסיס כתובת MAC במתג. ניתן להפעיל Port-Security באופן ספציפי על פורט בלבד, לא ניתן להפעיל את המנגנון בצורה גלובלית על כל המכשיר. Port-Security מתייחס לכתובת ה-MAC הרשומה כ-Source MAC ב-Frames שנכנסים לפורט. חשוב לציין שמנגנון זה מתייחס לתנועת Ingress בלבד - הכוונה היא רק לתנועה שנכנסת לפורט ולא תנועה שיוצאת ממנו.

אנו נגדיר Port-Security בעזרת הפקודות הבאות במערכת IOS של Cisco:

```
Switch(config)# interface f0/1
Switch(config-if)# switchport port-security
```

הגדרות אלו ידליקו את Port-Security עם הפרמטרים המוגדרים כברירת מחדל. ניתן לראות פרמטרים אלו באמצעות הפקודה הבאה:

```
Switch# show port-security interface f0/1
Port Security : Enabled
Port Status : Secure-down
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:0000.0000.0000:0
Vlan : 0
Security Violation Count : 0
```

כפי שניתן לראות, ישנם מספר פרמטרים נתונים שאנו יכולים לשנות או לכוונן. כעת נעבור על הפרמטרים האלו, נראה כיצד מגדירים אותם, ואז נראה את כל העניין בפעולה.

Violation Mode

Violation הוא מצב שבו מדיניות האבטחה שלו הופרה. למשל, אנו הגדרנו בעזרת Port-Security שרק מחשב A יכול להתחבר לרשת, ולפתע מישהו ניתק את A וחיבר במקומו את B. ה-Violation Mode נותן לנו את האופציה לבחור את הצורה שבה Port-Security יגיד במצב כזה. המצבים שהם ניתן להשתמש הם:

- Shutdown - ברגע שבו יתקבל בפורט Frame אשר הגיע מכתובת MAC לא מאושרת, הפורט ירד למצב err_disable. לא יהיה ניתן להשתמש בפורט עד שנדליק אותו בחזרה. זהו מצב ברירת המחדל.
- Protect - מצב זה יסנן Frames אשר הגיע מכתובת MAC לא מאושרת. Frames מכתובות מאושרות לא יושפעו.
- Restrict - מצב זה דומה בפעולתו לProtect, אך מודיע למערכת באמצעות הודעת Syslog על ההפרה, ומעלה את הViolation Counter.

ניתן לשנות את ה-Violation Mode בצורה הבאה:

```
Switch(config-if)# switchport port-security violation
restrict/protect/shutdown
```

Maximum MAC addresses

ניתן להגדיר ל-Port-Security מהו המספר המקסימלי של כתובות MAC שניתן ללמוד על פורט מסוים. מספר ברירת המחדל הוא 1. נגדיר את כמות כתובות ה-MAC אשר ניתן ללמוד בפורט בצורה הבאה:

```
Switch(config-if)# switchport port-security maximum 2
```

ניתן להגדיר כמות כתובות MAC שאותם הפורט יכול ללמוד גם לפני סוג ה-VLAN שאליה הפורט משויך. ניתן לשייך פורט ל-Access VLAN מסוימת ול-Voice VLAN אחרת. אנו יכולים להגדיר כמויות מקסימליות שונות ללמידה בסוגי ה-VLANS האלו:

```
Switch(config-if)# switchport port-security maximum 1 vlan access
Switch(config-if)# switchport port-security maximum 1 vlan voice
```

Mac Address Learning

ניתן להגדיר את הצורה שבה Port-Security לומד כתובות MAC. כמו עם רוב הדברים, ניתן לעשות את זה בצורה ידנית, או לתת ל-Port-Security ללמוד בצורה דינמית. ניתן להגדיר ל-Port-Security כתובות MAC באופן ידני בצורה הבאה:

```
Switch(config-if)# switchport port-security mac-address 001b.d41b.a4d8
```

כמובן שהפתרון הזה הוא לא יעיל במיוחד בסביבה עם תחנות רבות. ניתן להגדיר את Port-Security מצב Sticky, שהוא מצב ברירת המחדל, המאפשר למידה עצמאית של כתובות MAC. אנו חייבים לוודא שהתחנות המחוברות לרשת בעת ההגדרה הן באמת התחנות שאמורות להיות מחוברות.

```
Switch(config-if)# switchport port-security mac-address sticky
```

Mac Address Aging

דבר נוסף שאנו יכולים להגדיר הוא כיצד הכתובות יתיישנו, כלומר, תוך כמה זמן ובאילו תנאים הפורט ישכח את הכתובות ויחליף אותן בחדשות. מנגנון ההתיישנות מתחלק לשני סוגי Timers:

- Absolute - מצב ברירת המחדל. במצב זה הפורט ישכח את הכתובות תוך כמות הזמן שנגדיר לו. ברירת המחדל היא 0, שמשמעותה Infinite - הפורט לא ישכח את הכתובות אלא אם כן נמחק אותן ידנית.
- Inactivity - במצב זה הפורט ישכח את הכתובות לאחר X זמן של חוסר פעילות. כלומר שאם הגדרנו את הטיימר על 4 דקות, ובמשך 4 דקות לא התקבל Frame מכתובות מאושרת כלשהי, הכתובת תשכח וכתובת אחרת תוכל לתפוס את מקומה.

הגדרות:

```
Switch(config-if)# switchport port-security aging time 5
Switch(config-if)# switchport port-security aging type
inactivity/absolute
```

Auto Recovery

בכדי שלא נצטרך אופן ידני לגשת לכל פורט שנפל בגלל Port-Security במצב Shutdown ולהדליק אותו (אלא אם כן אנו רוצים למצוא את העובד הסורר ולנזוף בו!), אנו יכולים להגדיר מנגנון התאוששות אוטומטי, שידליק את הפורט בחזרה לאחר זמן מסוים. זמן ההתאוששות מוגדר בשניות:

```
Switch(config)# errdisable recovery cause psecure-violation
Switch(config)# errdisable recovery interval 600
```

במצב כזה, 10 דקות לאחר שפורט נפל, נקבל את ההודעה הבאה על כך שהפורט מנסה לעלות בחזרה:

```
%PM-4-ERR_RECOVER: Attempting to recover from psecure-violation
err-disable state on Fa0/13
%LINK-3-UPDOWN: Interface FastEthernet0/13, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13,
changed state to up
```

בואו נראה את זה בפעולה:

לאחר שחיברנו לפורט מחשב מסוים, נוכל לראות ש-Port-Security למד את כתובת ה-MAC:

```
Switch# show port-security interface f0/1
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address: 001b.d41b.a4d8:10
Vlan :  01
Security Violation Count : 0
```

ברגע שננתק את המחשב, ונחבר במקומו מחשב אחר, נקבל את ההודעה הבאה המעידה על הפרת המדיניות:

```
%PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1,
putting Fa0/1 in err-disable state
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 0021.55c8.f13c on port FastEthernet0/1.
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
```

לאחר מכן נוכל לראות שהפורט מצב Err_disable, בהנחה שהיינו על מצב Shutdown. ושה-Violation Counter עלה:

```
Switch# show port-security interface f0/13
Port Security : Enabled
Port Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0021.55c8.f13c:10
Security Violation Count : 1

Switch# show interfaces f0/13
FastEthernet0/13 is down, line protocol is down (err-disabled)
Hardware is Fast Ethernet, address is 0013.c412.0f0d (bia
0013.c412.0f0d)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
...
```

לסיכום

אין ספק ש-Port-Security הוא לא פתרון מושלם לאבטחת הרשת שלנו ב-Layer 2, אבל הוא ללא ספק אחד שצריך להכיר.

על המחבר

רון הרניק (CCNP) הוא מדריך לנושאי תקשורת נתונים במכללת IITC ברמת גן, ומחבר הבלוג The Ping Factory. בנוסף, הוא משתדל לציית לכל הסטראוטיפים המאפיינים את החנון הטיפוסי.

כתובת אימייל ליצירת קשר:

ronh@iitc.co.il