FireWall Hacking

cp77fk4r

מסמך זה הורד מהאתר http://www.underwar.co.il.

על סדר היום:

I - הקדמה.

II - Ack Tunneling.

III - HolyGirl DoS Attack.

IV - Config it!.

V - OtherStuff.

VI DMZ - and Raw Socket.

VII - סיכום.

I - הקדמה:

הדעה הרווחת היא שטכנולוגיית ה-Fiewall מסוגלת לאבטח לגמרי את מחשבכם, אם אתם חוששים למידע הרגיש שנמצא עליו ולכן ישר ממליצים לכם להתקין Firewall מסוים.
זה אכן טוב לשים Firewall, אך שום דבר בעולם אינו מושלם, וגם ה-Firewall והאבטחה שהוא מספק אינם מושלמים.

בטקסט זה אני אסקור מספר דרכים שהאקרים משתמשים בהן בשביל לעקוף את אבטחתו של ה-Firewall בכדי להכנס (או לצאת!) למערכת שעליה הוא מגן. קריאה מהנה.

II - Ack Tunneling:

אז מה זה בכלל Tunneling Ack? נתחיל ראשית בהסבר קצר מה זה **Ack**:
על מנת ליצור תקשורת TCP-Client/Server בין שני מחשבים, אנחנו צריכים לעבור מספר שלבים:

I) הClient שולח פאקט עם דגל Syn לServer בכדי להגיד לו שהוא רוצה לפתוח בתקשורת.

II) הServer בשביל לאשר את הבקשה, שולח כתגובה פאקט בעל שני דגלים, אחד שלAck ואחד של Syn לClient.

III) הClient שולח פאקט יחיד בעל דגל Ack לServer בכדי להגיד לו שהאישור התקבל.

זהו בעצם האלגוריתם HandShake Three Way שבו משתמשים לתקשורת בTCP.

IV) ישנו את החלק הרביעי שהוא שליחת פאקט עם דגל Fin שאומר שכל המידע נשלח- ומאפשר לסגור את הקשר, החלק הזה קיים, אבל לא נחשב כחלק מיצירת קשר, אלא כסיומו.

כיצד נושא זה מתקשר לאבטחת Firewall? אני בטוח שרב מי שקינפג בחייו פיירוול נתקל ב-Syn Blocking.
רב הפיירוולים, כשקובעים להם לחסום גישת מידע מאנשים שמנסים ליצור קשר עם קבצים הקיימים במחשב שלכם או אפילו קבצים מהמחשב שלכם שמנסים ליצור קשר עם העולם החיצון- ואין להם אישור יחסמו, איך הפיירוול חוסם אותם? הוא פשוט בודק אם הפאקט שנשלח הוא בעל Syn, ואם כן- הוא לא נותן לו לצאת/להגיע למערכת, וככה הוא חוסם את התקשורת, כך שאם מדובר למשל בטרויאן- אותו פורץ שמנסה לתקשר עם ה-Server שהותקן על המחשב שלכם- לא יצליח, וככה הפיירוול מנע את החדירה והגן על המחשב ועל המידע שלכם.

כאן נכנס הקטע של ה-Ack Tunneling.
על מנת להצליח לשלוט על המחשב שלכם, על אותו פורץ להצליח לתקשר עם ה-Server שהוא שתל במחשב שלכם דרך הפיירוול, אבל הפיירוול מונע ממנו לפתוח בחיבור ע"י כך שהוא מונע מה-Syn להגיע למערכת. הפתרון לבעיה: לא משתמשים ב-Syn! פשוט כך, מבססים את המידע שרוצים לשלוח רק בפאקטים בעלי דגל Ack.
הפיירוול לא מוגדר להתעסק עם פאקטים כאלה, בשביל שדרכי התקשורת שהמשתמש כן רוצה וכן מאשר כן יכלו להפתח, ולכן הוא לא ימנע מאותן חבילות מידע לעבור מעבדו.

אי אפשר להגדיר תקשורת כזו כ-TCP מכיוון שלא בוצעו שלושת השלבים שבה, אבל היא עדיין מסוגלת להעביר מידע בין מחשב, וזה מה שחשוב.

Arne Vidstrom כתב טרויאן בשם AckCmd בכדי להמחיש זאת, אני לא מעודד אתכם להשתמש בטרויאנים, אני רק מעודד אתכם ללמוד את הרעיון, הטרויאן מאפשר לקבל CmdShell של אותו מחשב גם אם הוא משתמש ב-Firewall

HolyGirl DoS Attack - III:

HolyGirl DoS Attack היא התקפה המבוצעת על הפיירוול.
המושג DoS אינו מתייחס כמובן אל מערכת ההפעלה בשם זה, אלא אל המושג Denial Of Service. מדובר כאן בהתקפות שמבצעים על מטרה מסוימת בכדי להציף אותה במידע עד שהיא קורסת/מושבתת.
לדוגמא, בהינתן שרת מסוים, נוכל לנסות לשלוח לו הרבה מאוד מידע עד שהוא קורס מרוב עומס הודעות- וככה אנחנו נפיל ונחסום את הגישה אליו.

ישנם סוגים רבים מאוד של התקפות DoS, כולן שונות וכולן מתבצעות בצורות שונות זו מזו, אבל לכולם בסיס אחד- הצפה, בכולם התוקף מנסה לתקוע ולהשבית ישום מסוים ע"י הצפתו.
התקפת הDoS הנקראת HolyGirl Attack, היא התקפה שבא התוקף/התוקפים מנסים להתחבר לכמה שיותר יציאות (Ports- פורטים) על השרת, מכמה מחשבים ביחד, ולהתנתק, ולהתחבר שוב, ולהתנתק וכו', מה שקורה זה בעצם שיש לנו פיירוול על השרת שאחראי על בדיקת המידע שנכנס דרך אותם הפורטים- אם נבצע התחברות אחת, הפיירוול יצליח לעמוד בקצב, אבל אם נתחבר- נשלח מידע- ונתנתק הרבה מאוד פעמים, הפיירוול בסוף ינצל את מירב הכח מעבד שהוקצב לו מראש- ויקרוס.

ישנם פיירוולים שינסו לבצע SelfReboot, ולכן אם נתקלנו בפיירוול בעל תכונה כזאת- יש לנו פרק-זמן קצר יחסית לבצע את הפעולות שאנו רוצים לבצע לאותו מחשב.
ישנה גם אפשרות שהאחראי על האבטחה באותה המערכת כתב סקריפט מסוים שאחראי על ניטור הישומים ובדיקה אם ישום הפיירוול נסגר בצורה מסוימת- ואם כן, לנסות לחכות מספר שניות ואז להריץ אותו שוב.
ניתן לכתוב סקריפט כזה בקלות, ולכן משתמשים בו במקומות רבים. פורץ הנתקל במצב כזה נאלץ לנסות לאתר את אותו הסקריפט ולהשמיד אותו.
דרך מאוד יעילה ונפוצה היא להריץ את ה-TsKill עם ה-ID של אותו הסקריפט- או פשוט עם הארגומנט "Wscript.exe" ולאחרי מכן, בכדי שנהיה בטוחים גם עם הארגומנט "Cscript.exe".

IV- Config it!:

"באג" נוסף שקיים בהרבה תוכנות פיירוול הוא הנגישות לקינפוג של ה-Firewall, מה הכוונה? לא מדובר פה בכשל אבטחה או משהו, אני מתכוון שמתכנתי אותו הישום אפשרו לשנות ולקנפג את הפיירוול בקלות יתר, בלי כל השגחה, ככה שכל אחד יכול לעשות זאת. הסכנה: האקרים יכולים לנצל את זה- ופשוט להוריד את כל האפקטיביות של הפיירוול,

מספר דוגמאות: הדוגמאות שאתן יהיו מהפיירוול החדש והמשוכלל שחברת Microsoft כ"כ התגאו בו, כמו שהם יודעים לעשות טוב מאוד.
מצד אחד, נראה שאין כל רע בקלות הקינפוג וידידות למשתמש- ולהפך, זה ניראה אחלה של דבר, אבל בכל זאת, זה מסוכן ביותר. אם לדוגמא, יצרנו טרויאן קטן, ואנחנו רוצים שהוא יוכל לגשת לאינטרנט גם במחשבים ש"מוגנים" בעזרת הפיירוול של ה-SP2, פשוט נוכל לקנפג את הפיירוול בעזרת פקודה אחת, פקודה שתאפשר לטרויאן שלנו גישה חופשית לאינטרנט- בלי שהפיירוול יפריע לו, פשוט מאוד, לפני שהטרויאן יוצר את הקשר עם הסייברספייס, או אפילו כל פעם שהמחשב נדלק, נגיד לו לכתוב ככה:

= Netsh firewall set allowedprogram program = [Path] name
SomeName] mode = ENABLE scope = ALL profile = ALL]

הפקודה הזאת אומרת לפיירוול של הווינדוס, להוסיף את הטרויאן שלנו לרשימת התוכנות שמורשות לגשת לנט- ה"תוכנות הבטוחות", וזהו, הוא יוכל לגשת לנט, לשלוח ולקבל פקודות ומידע, והפיירוול ישב בשקט ולא ינסה לעצור אותנו, ככה זה, יש יותר פשוט מזה? אני ממש ממש לא בטוח.

טיפ קטן: ה[SomeName] יכול להיות כל שם, אבל עדיף לכתוב שמות שיראו אמיתיים ולא מחשידים, שיראו כל מני שירותים של הוינדוס, למשל Firewall Windows Service או Windows Security Update או דברים שלא יחשידו את מי שיבדוק ברשימת הפורטים והתוכנות המורשות לגשת בחופשיות לאינטרנט, אני סומך על הדמיון שלכם.

דוגמא שניה היא פשוט להגיד לגרום לתוכנה שלנו לכתוב את הפקודה הבאה בכל פעם שהיא רוצה לגשת לאינטרנט- או (מה שיותר כדאי) זה לגרום למחשב להריץ את הפקודה הזאת בכל פעם שהוא נדלק/מתחבר לנט/מריץ את הפיירוול.
הפקודה היא:

Netsh firewall set portopening TCP [Port] ENABLE

פשוט, בעזרת הפקודה הזאת אנו יכולים לקנפג את הפיירוול כך שיוסיף פורט מסוים שאנו רוצים (הפורט שהטרויאן שלנו משתמש לדוגמא) שכשתוכנה מסוימת תרצה לפתוח אותו- הפיירוול יאפשר לה לפתוח אותו בלי לגרום לבעיות, פשוט מאוד, אין סיבה שהפיירוול החדש של מייקרוסופט יפריע לנו בתור אנשים נחמדים שלא רוצים להזיק- וגם בתור אנשים "קצת" אחרים...
שוב, גם פה, כדי לפתוח/להשתמש בפורטים שלא יחשידו את האחראי אבטחה או את מי שיבדוק ברשימת הפורטים המורשים להפתח.
ישנם עוד הרבה ישומי פיירוול בעלי התכונה הזאת, פשוט צריך לחפש טיפה מהן הפקודות המתאימות, לרב הן באות ביחד עם ההתקנה- באיזה קובץ ReadMe או Help...

משהו נוסף: כמובן שאת הפקודות האלה אפשר לבצע רק ע"י משתמש שהורשה לקנפג את הפיירוול מהחשבון שלו, רב המשתמשים "הביתיים" גולשים מהחשבון של האדמין והשאר- אפשר בקלות להוסיף סקריפט קטן לטרויאן שלנו שיבדוק אם המשתמש הוא Administrator או משתמש אחר בעל "גישת קינפוג" ואם כן- להריץ את הפקודה, במערכות מבוססות NT השם משתמש שמור תמיד במשתנה %USERNAME%, ואת קבוצות המשתמשים אפשר להשיג ע"י הפקודה Net User.

אם ממש רוצים- אפשר גם לבנות סקריפט שיחכה שיתחברו מהחשבון של האדמין- וכשיתחברו משם לאפשר לכל החשבונות לקנפג את הפיירוול וככה שמאז- כל פעם שיתחברו יהיה אפשר לקנפג את הפיירוול, ולא משנה איזה משתמש זה, אני בטוח שאתם יכולים לחשוב על עוד הרבה דברים בכדי לעקוף את הבעיה הקטנה הזאת, ולכן אני לא אמשיך לפרט.

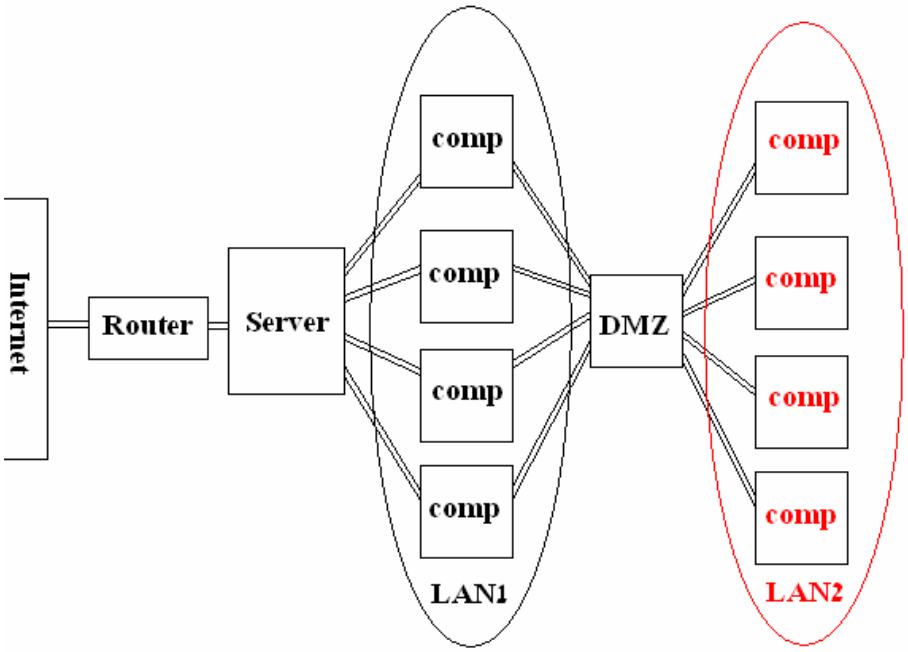
V - OtherStuff:

הבאגים/דרכי ביצוע שהסברתי עליהם בפרקים הקודמים לא קיימים בפיירוולים ספציפים (חוץ מהדוגמאות שנתתי- שאם הם היו מפיירוול ספציפי נתתי את שמו), אבל קיימים גם באגים בכל מני פיירוולים ספציפים, ואחת הדרכים בהם משתמשים פורצים היא לפני נסיון הפריצה – גילוי של כמה שיותר מידע עליו, וחלק מהמידע הוא כמובן גם באיזה אמצעים המטרה מגנת ומאבטחת את עצמה כנגד פורצים. ישנם דרכים לגלות איזה פיירוול מאבטח את המערכת המסוימת, בכדי לדעת באיזה פיירוול מדובר- אפשר כמובן גם להשתמש בהנדסה חברתית, אבל אפשר גם על-ידי משחק קלט/פלט עם השרת לדעת באיזה פיירוול מדובר, אם למשל אנחנו יודעים על באג שהיה קיים בפיירוול של CheckPoint, שהיה קיים ב Config Remote- שהיה אפשר להתחבר אליו בפורט מסוים שקבעו- ועם סיסמא לשנות כל מני דברים בו. נכון שהיה צריך סיסמא והכל, אבל למי שרק רוצה לחקור את המערכת ולאסוף מידע זה הספיק - הוא היה סורק פורטים, מנסה להתחבר דרך הפורט שהאחראי אבטחה קבע בשביל ה-Remote Config ואז הוא מקבל את הבאנר של ה"ברוכים הבאים ל Service Remote Config של הפיירוול של CheckPoint ובלה בלה בלה". אומנם הפורץ לא יודע את הסיסמא, אבל עכשיו הוא יודע איזה פיירוול מאבטח את המערכת הזאת. ידע זה מסוכן, מכיוון שבדיוק באותה מערכת פיירוול היה באג, שאם הפיירוול היה מקבל פאקט בחיבור UDP שנותב לפורט מספר 0 הוא לא היה יודע איך להגיב ומה לעשות- והיה מתחיל להשתגע ואחרי כמה שניות- היה קורס. נכון, היה לו מערכת שמבצעת SelfReboot אבל עדיין-זהו אכן באג רציני.

הדגש הוא אינו על הבאג הספציפי הזה, אלא הדגשת העובדה כי ניתן לחקור את המערכת- לנסות לגלות באיזה אמצעי אבטחה הם משתמשים- ואז לחפש בו באגים וחורי אבטחה שקיימים בה.

Socket - V.I DMZ and Raw:

דוגמא נוספת הינה הפיירוול PIX, בו יש אפשרות לנהל DMZ (Demilitarized Zone) מחשב שנקרא **DMZ**, הוא מחשב שמקשר בין שני רשתות, רשת פנימית ורשת חיצונית, תסתכלו עת הציור הבא:



הרשת השחורה ("LAN1"), היא רשת חיצונית- שיש אליה גישה לנט בצורה חופשית, אפשר לשים עליה אתרים, לאכסן קבצים, ודברים כאלה.

הרשת האדומה ("LAN2"), היא רשת פנימית, בתוכנה החברה (או הגוף שברשותו היא קיימת) משתמש בכדי לאכסן את קבצי החברה או שאלה אפילו מחשבי העובדים של החברה- המחשבים שהם עובדים איתם בעבודה.

עכשיו, מצד אחד- המחשבים האלה גם צריכים גישה לאינטרנט, אבל מצד שני הם גם צריכים הרבה מאוד אבטחה, זהו שיקול שדורש הרבה מאוד מחשבה.

בדיוק בגלל זה קיים השירות DMZ, שזהו שירות שמתקינים על מחשב (עדיף שלא בשימוש)- והוא השער בין הרשת החיצונית/האינטרנט, השירות הזה צריך להיות מאוד מאובטח וכמובן מאוד יציב, הוא צריך לבדוק בקפידה כל מידע ומידע שעובר דרכו, פנימה והחוצה, ועדיין להצליח לעמוד בקצב ולהיות מספיק מהיר.
ובפיירוול PIX של חברת CISCO ישנה אפשרות כזאת, שהוא ישמש כאחראי על מערכת DMZ.
באותו השירות הזה, יש גם באג, אם נפרוץ לרשת מסוימת- וניראה שהיא מחוברת לרשת פנימית ומוגנת בעזרת DMZ מסוים, ונגלה בצורה כלשהי- שמדובר בשירות של PIX נוכל לנצל את הבאג. אסביר עליו כעת:
כשמשתמשים ב-PIX כ-DMZ מסוים הוא כמובן יבצע לוג של כל המידע שעובר דרכו, וכמובן ינהל ויהיה אחראי על כל החיבורים שיעברו דרכו, ואם הוא יקבל
פאקט בעל דגל RST בחיבור TCP מסויים- הוא כמובן ינתק את החיבור, עכשיו, ישנה אפשרות ע"י תכנות בRaw Socket ליצור פאקט בצורה כזאת:

Header: Tcp
Source ip: Server של ה IP
ip: DMZ Destination של ה IP
Source port: Server הפורט שדרכו ה DMS מחובר ל
port Destination: כמו הקודם
Flag: RST

אם נבצע שליחה לPIX- הוא יחשוב שמדובר בחיבור שלו עם הסרבר (כמובן שזה יכול להיות כל מחשב שמחובר אליו _באותו הזמן_) והוא ינתק איתו את החיבור, וכמובן שבאותו הרגע גם לנו לא יהיה חיבור איתו, כי היינו מחוברים אליו דרך האינטרנט שהגיע אליו דרך השרת, אנחנו אומנם לא משיגים בעזרת זה גישה, אבל אנחנו מבצעים כאן ללק ספק DoS Attack יפה במיוחד.
ההתקפה הזאת די ישנה, אבל הייתה קיימת בהרבה מהגרסאות שהיו בפיירוול של חברת SISCO.

VI - סיכום:

ישנם עוד הרבה מאוד באגים, גם ספציפים לישום פיירוול מסוים, וגם כאלה שקיימים בכמה ישומי פיירוול שנכתבו בצורה דומה חלקית, אני מאוד מקווה שנהנתם לקרוא ושהבנתם את כל מה שנכתב, חשבתי לכתוב טקסט מיוחד על שירותי DMZ אבל אני לא בטוח, נראה בעתיד, בכל אופן, אני מאוד מקווה שהבנתם את מה שרציתי להעביר דרך הטקסט הזה, נכון שפיירוולים עוזרים ומאבטחים את המחשב- אבל שום טכנולוגיה שנכתבה ע"י בני אדם היא, "בלתי פריצה" או "מאבטחת לגמרי" וכו', כי כמו שראיתם- קיימים הרבה חורים, והרבה בעיות יתגלו בעתיד, ככה שתשתמשו בפיירוולים כמובן, אבל אל תרגישו חסיני-כל.

מאוד מקווה שנהנתם לקרוא את הטקסט ושלמדתם דברים חדשים.