תרגיל בית 5 - תיעוד יבש

הוראות הרצה:

כדי להפעיל את ה-firewall:

./src/module/sudo insmod firewall.ko

./src/interface/main load_rules ./[rules_file_name]

כדי להפעיל את שרתי הפרוקסי:

./src/proxy/http_proxy_server.py

./src/proxy/ftp21_proxy_server.py

./src/proxy/ftp21_proxy_server.py

./src/proxy/smtp_proxy_server.py

user interface:

activate - הפעלת חומת האש

deactivate - כיבוי חומת האש

show_rules - הצגת את רשימת החוקים העדכנית

clear_rules - מחיקת את רשימת החוקים

load_rules <path> - טעינת רשימת חוקים מקובץ

show_log - הצגת רשימת תיעוד של פעילות חומת האש

clear_log - מחיקת רשימת התיעוד

show_connection_table - הצגת טבלת החיבורים העדכנית

הסבר על הקוד:

המודול -

המודול מורכב מ-4 רכיבים -

1. **רכיב תקשורת (netfilter) -** נרשם ל-2 hook-ים: PRE-ROUTING, OUTPUT ומנטר את הפקטות ומקבל את החלטות הניתוב.
2. **רכיב חוקים -** מחזיק טבלה סטאטית בגודל 50 המכילה את חוקים (טיפוס struct מסוג rule_t) שמנהל הרשת מזין.
3. **רכיב חיבורים -** מחזיק רשימה מקושרת דינמית (טיפוס struct מסוג conn_t) המנהלת את החיבורים הקיימים ותקינותם, עבור הפרוטוקולים http, ftp.
4. **רכיב לוג -** מחזיק טבלת סטאטית בגודל 1000 המכילה לוגים (טיפוס struck מסוג log_row_t) המתעדים את החלטות הניתוב.

בפונקציית טעינת המודול [init_module] כלל הרכיבים מאותחלים - נפתחים שלושה sysfs device-ים עבור רכיבים 2-4.

בפונקציית ניקוי המודול [cleanup_module] הרכיבים מנוקים - מבוטלת ההרשמה לה-hook-ים ונסגרים שלושת ה-sysfs device.

כשעושים init למודול, ה-firewall נדלק אוטומטית - כלומר כל חבילה שתעבור מרגע העלייה, תעבור דרך הפונקציות שהגדרתי.

שרתי הפרוקסי -

בניתי 4 שרתים - שרת לתקשורת HTTP, שרת לתקשורת FTP21, שרת לתקשורת FTP20 ושרת לתקשורת SMTP. כל שרת מאזין לפורט מוגדר מראש (עושה bind) ואת התקשורת מול הצד השני עושה ע"ג פורט אקראי לכל התקשרות (הפורט של כל התקשרות נשמר ברשימת החיבורים הדינאמיים בתא מיוחד כדי שאוכל לנתב לפורט הזה את התשובות)

[בהגדרה אצלי השרתים יושבים מחוץ לרשת הפנימית, כלומר פנייה לשרת HTTP,FTP21,SMTP היא רק פניה מתוך הרשת החוצה והיא מנותבת לפורטים המוגדרים מראש בהתאם לפרוקסי המתאים. רק במקרה של תקשורת FTP20 הפנייה הראשונה מתבצעת לתוך הרשת שלנו ורק במקרה הנ"ל מופנית לפורט המוגדר מראש של הפרוקסי הנ"ל, והתקשורת של הלקוח מול הפרוקסי מתבצעת ע"ג פורט רנדומלי]

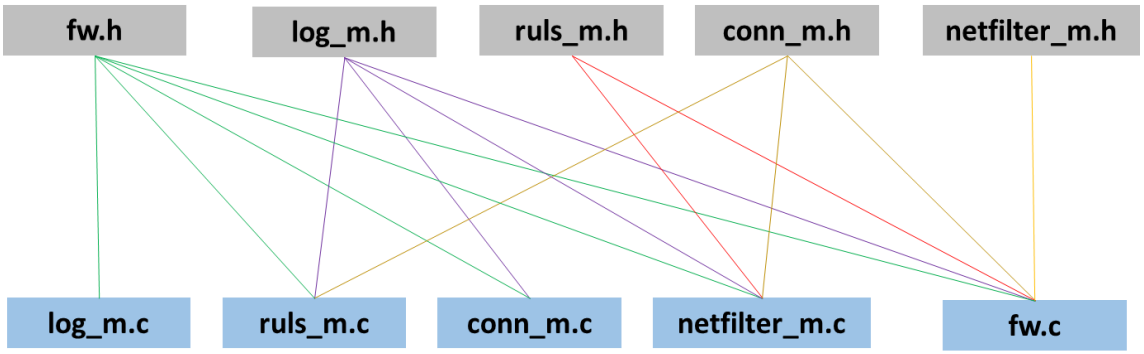
[התייחסות ל-dlp מופיעה בשקפים שהצגתי בכיתה ואת סינון החולשה שלי עשיתי פשוט ע"י זיהוי פקודת ה-GET שיוזמת את התקיפה וחסימתה - כמו שאמרתי בכיתה]

ממשק ניהול המערכת - בהתאם לפקודה שמוזנת ע"י מנהל הרשת, מתבצעת הירשמות ל-attribute המתאים והפקודה הרצויה מתבצעת.

סכימת מודול ה-firewall - משתמשת בשלושה char device בעלי sysfs class משותף ו-sysfs device נפרדים.

Char Device	Sysfs Class	Sysfs Device	Device Attributes	Attribute Functions
fw_log	fw	fw_log	log_size	(display) return_log_size (modify) -
			log_clear	(display) clear_log (modify) show_log
fw_rules	fw	fw_rules	active	(display) check_if_on (modify) turn_on_off
			rule_size	(display) num_of_rules (modify) clear_rules
			rule_management	(display) display_rules (modify) load_rules
fw_conns	fw	fw_conn_tab	conns	(display) display_conns (modify) close_connection
			proxy	(display) send_conn_data_to_proxy (modify) recive_conn_data_from_proxy

תלויות בין קבצי ה-fw:



בדיקת הפקטות -

ברירת המחדל שלי לגבי פקטות היא לדחות אם אין התאמה לחוקים שהגדיר מנהל הרשת.

כאשר פקטה נקלטת באחד ה-hook-ים, נתוני הניתוב השונים נשלפים ממנה ואז מתבצעת ההחלטה:

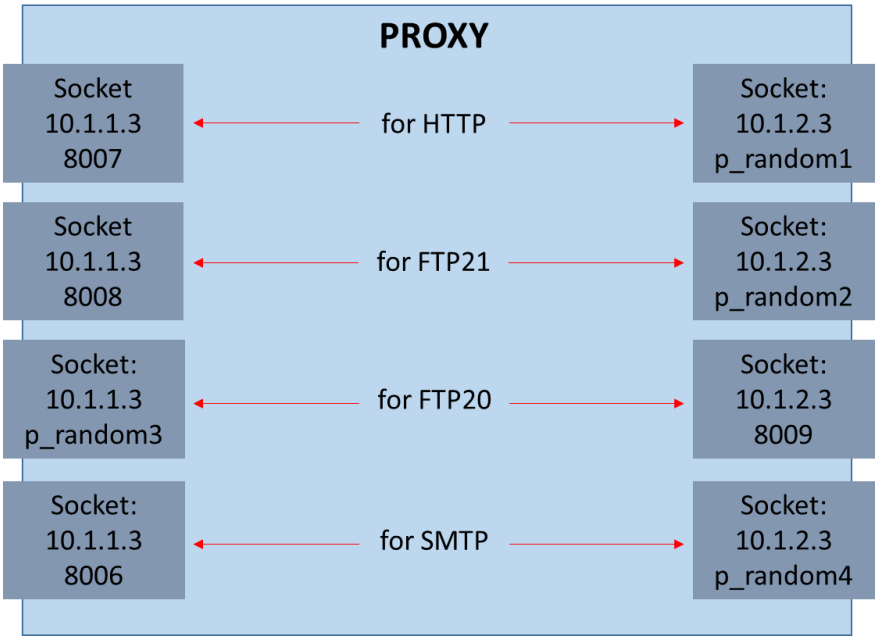
1. אם הפרוטוקול אינו TCP מתבצעת בדיקה מול טבלת החוקים הסטאטיים ואם היא מתאימה לאחד החוקים פועלים לפי מה שמוגדר בחוק. אחרת, אם היא לא מתאימה לאף חוק, היא נפסלת.
2. אם הפרוטוקול הוא TCP ו-
   a. זאת פקטת SYN - מתבצעת בדיקה מול טבלת החוקים הסטאטיים ובמידה והפקטה מאושרת מתווספת שורה חדשה לטבלת החיבורים הדינמיים והפקטה מאושרת.
   b. זאת לא פקטת SYN - מתבצעת בדיקה מול רשימת החיבורים הדינמיים ואם היא שייכת לחיבור קיים והסטאטוס שלה נכון היא מאושרת.

הרשומות ברשימת החיבורים:

- כאשר פקטת SYN נקלטת ב-prerouting והיא מאושרת מבחינת טבלת החוקים הסטאטיים, מתווספת רשומה חדשה לרשימת החיבורים הדינאמיים כאשר הנתונים בה הם בהתאם לסדר הנתונים בפקטה - כלומר src_ip=packet src_ip...
- כאשר פקטת SYN נקלטת ב-output, מתבצע חיפוש ברשימת החיבורים הדינאמיים לפי נתוני היעד שלה ואם נמצאת התאמה ז"א שזאת תקשורת תקינה, נתוני הפקטה מזוייפים "בחזרה" לנתונים שאמורים להיות כלפי חוץ ואז מתווספת רשומה חדשה לרשימת החיבורים הדינאמיים אך הנתונים שלה הם בכיוון הפוך לסדר הנתונים בפקטה - כלומר src_ip=packet **dst**_ip...
- כלומר התקשורת של הלקוח הפנימי מול הפרוקסי נבדקת מול טבלת החיבורים כאילו כולה בכיוון היציאה והתקשורת של הפרוקסי עם השרת נבדקת מול טבלת החיבורים כאילו כולה היא בכיוון הכניסה. כלומר, כל תקשורת שנקלטת ב-prerouting היא כבר בסדר שצריך לבדוק וכל התקשרות שנקלטת ב-output צריך להיבדק כאילו היא הפוכה בסדר שלה. [המחשה אחרי הפסקה הבאה]
- ת"ל שבמקרה של תקשורת ftp20 זה בדיוק הפוך. [שוב, המחשה אחרי הפסקה הבאה]

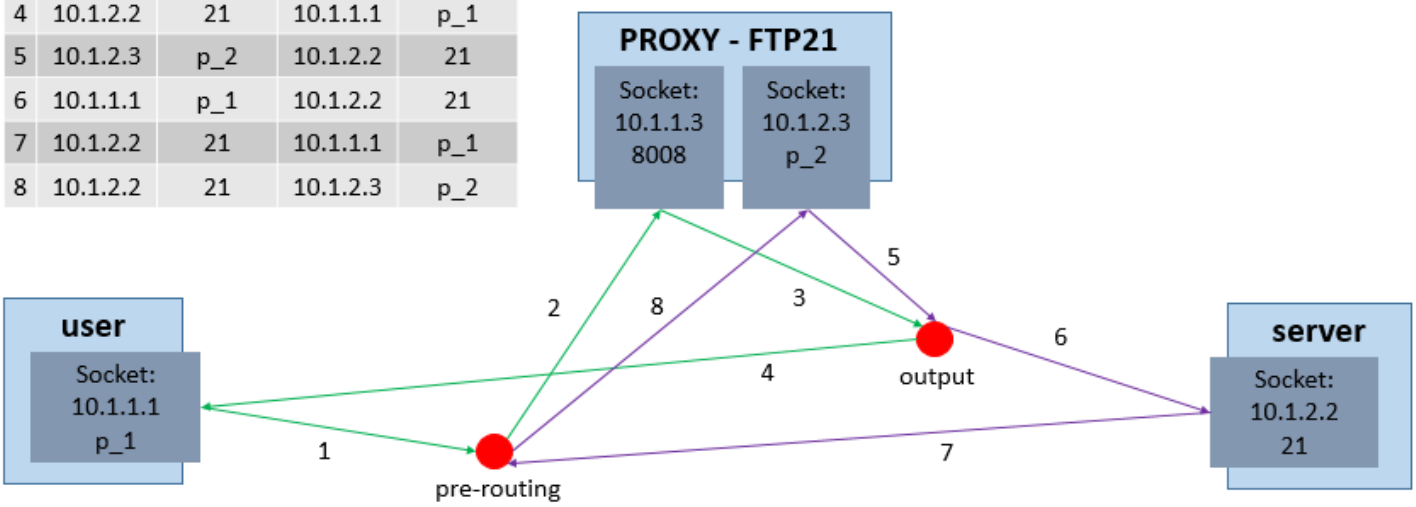
זיופי פקטות בפרוטוקול TCP:

- כאשר פקטה נתפסת ב-prerouting היא קודם נבדקת ברשימת החיבורים הדינמיים ואז מזוייפת (כי טבלת החיבורים מכילה את הנתונים האמיתיים)
- כאשר פקטה נתפסת ב-output היא קודם מזוייפת בחזרה לנתונים האמיתיים ואז נבדקת ברשימת החיבורים הדינמיים. (אני בודק פקטות גם ב-output כדי לוודא לחיצת יד תקינה והתנהלות תקינה מול השרת)



	src_ip	src_port	dst_ip	dst_port
1	10.1.1.1	p_1	10.1.2.2	21
2	10.1.1.1	p_1	10.1.1.3	8008
3	10.1.1.3	8008	10.1.1.1	p_1
4	10.1.2.2	21	10.1.1.1	p_1
5	10.1.2.3	p_2	10.1.2.2	21
6	10.1.1.1	p_1	10.1.2.2	21
7	10.1.2.2	21	10.1.1.1	p_1
8	10.1.2.2	21	10.1.2.3	p_2

Connections Table			
src_ip	src_port	dst_ip	dst_port
10.1.1.1	p_1	10.1.2.2	21
10.1.2.2	21	10.1.1.1	p_1



*(הדוגמא מעל, זהה במקרים של הפרוסי של HTTP ו-SMTP רק בהבדלי הפורטים המוגדרים מראש)

	src_ip	src_port	dst_ip	dst_port
1	10.1.2.2	20	10.1.1.1	p_1
2	10.1.2.2	20	10.1.2.3	8009
3	10.1.2.3	8009	10.1.2.2	20
4	10.1.1.1	p_1	10.1.2.2	20
5	10.1.1.3	p_2	10.1.1.1	p_1
6	10.1.2.2	20	10.1.1.1	p_1
7	10.1.1.1	p_1	10.1.2.2	20
8	10.1.1.1	p_1	10.1.1.3	p_2

Connections Table			
src_ip	src_port	dst_ip	dst_port
10.1.2.2	20	10.1.1.1	p_1
10.1.1.1	p_1	10.1.2.2	20