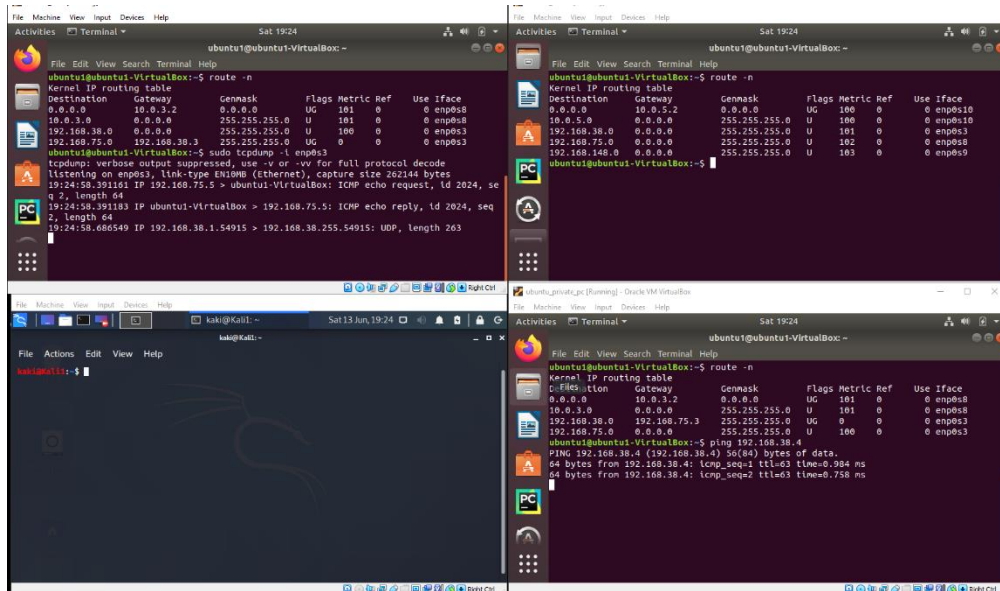


אבטחת תקשורת - תרגיל 2

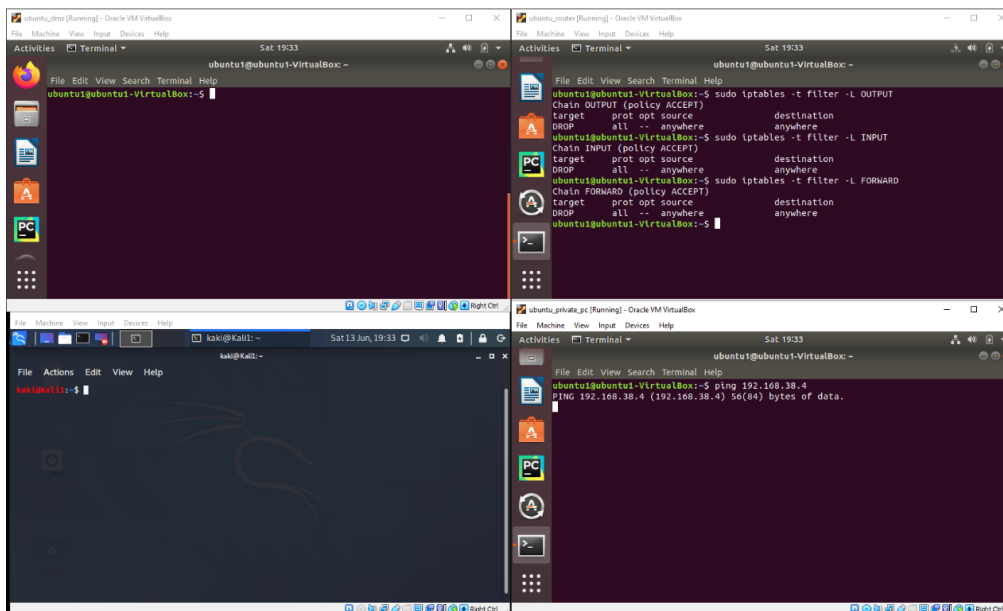
ב. בסעיף זה יישמנו מדיניות whitelisting אשר חוסמת את כל התעבורה בין הרשתות השונות דרך הראטר בעזרת iptables.

ראשית, מנענו תעבורה בטבלאות ה-input/output של הראטר כיוון שאף גורם לא אמור לפנות אליו בצורה כזאת. לאחר מכן מנענו תעבורה של טבלת ה-forward כדי למנוע את התעבורה דרך הראטר כנדרש בסעיף זה.

לפני (יש תקשורת בין private pc – dmz):



אחרי whitelisting (ניתן לראות את החוקים וההגדרות בהם השתמשנו בתמונת המסך בחלק הימני עליו):

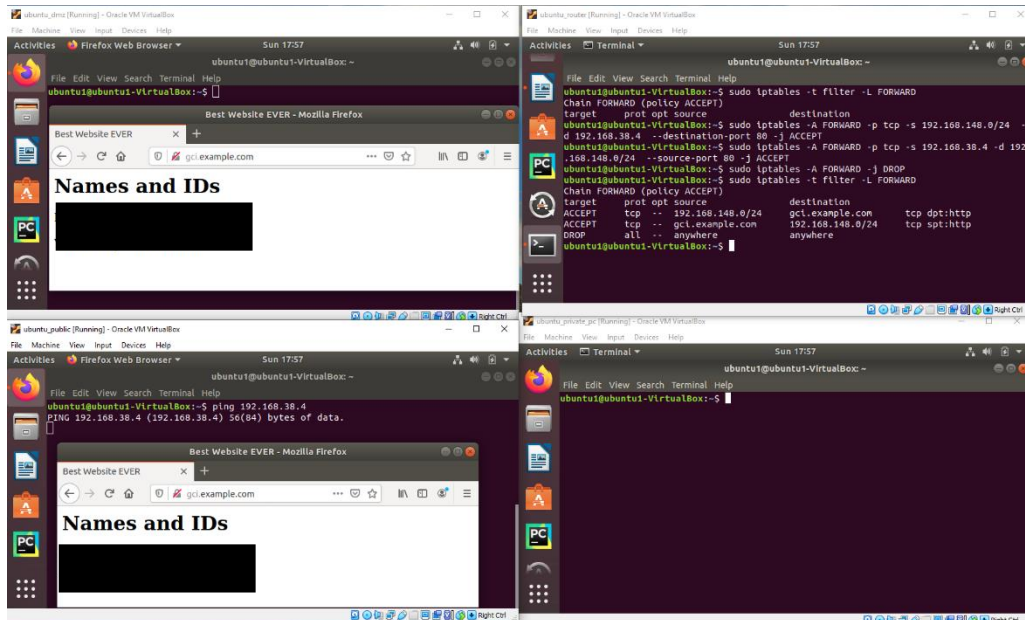


ג. (החלפנו את kali לubuntu בשביל הנוחות).

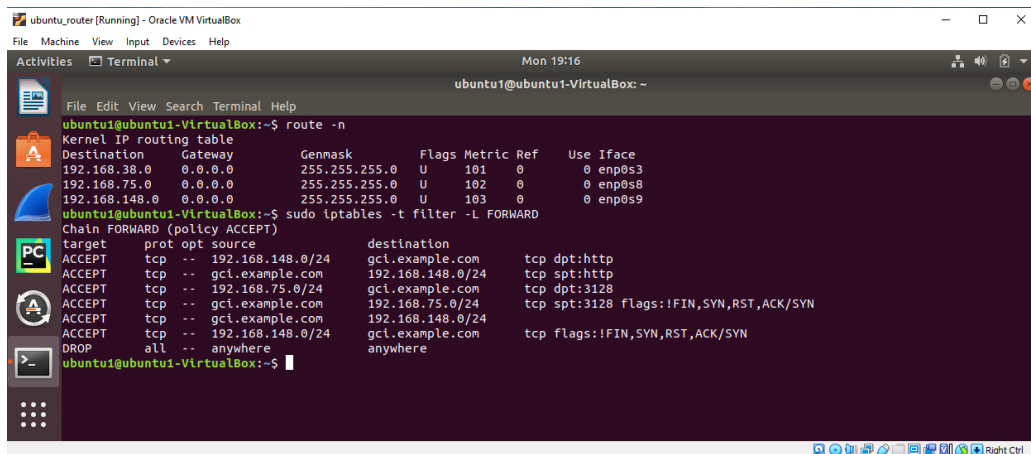
הסרנו את הגדרת ה-DROP מה-IPTABLES כדי להחזיר אותה בסוף הטבלה. הוספנו הגדרה שמאפשרת תקשורת TCP מרשת D לפורט 80 ברשת B.

הוספנו הגדרה שמאפשרת תקשורת TCP מפורט 80 ברשת B לרשת D.
כל שאר האפשרויות ייחסמו על ידי ה-firewall.

ניתן לראות שניתן להיכנס לאתר האינטרנט שיצרנו ברשת B, ברשת D (שמאל למטה), אך לא ניתן לקבל ping מהקו של המחשב שעליו נמצא השרת, כנדרש בסעיף זה.

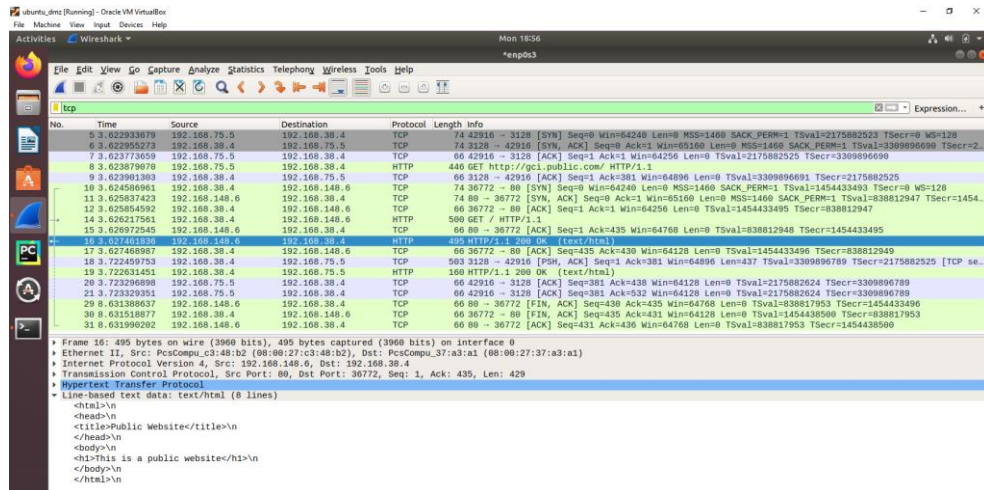


- ד. ניתן לראות את החוקים שהוספנו לטבלת הFORWARD בתמונה המצורפת.
- שורה 3: תקשורת ממחשבים ברשת A לשרת הפרוקסי על פורט יעד 3128 (פרוקסי) בלבד.
- שורה 4: תקשורת משרת הפרוקסי למחשבים ברשת A על פורט מקור 3128 בלבד, ללא הרשאת הקמת חיבור (SYN).
- שורה 5: תקשורת מהפרוקסי (על רשת B) לרשת D (פתחתי שרת אינטרנט בד).
- שורה 6: תקשורת מחשבים מרשת D ללא הרשאת הקמת חיבור (SYN) אל הפרוקסי.
- שורה 7: זדוק כל תקשורת אחרת.



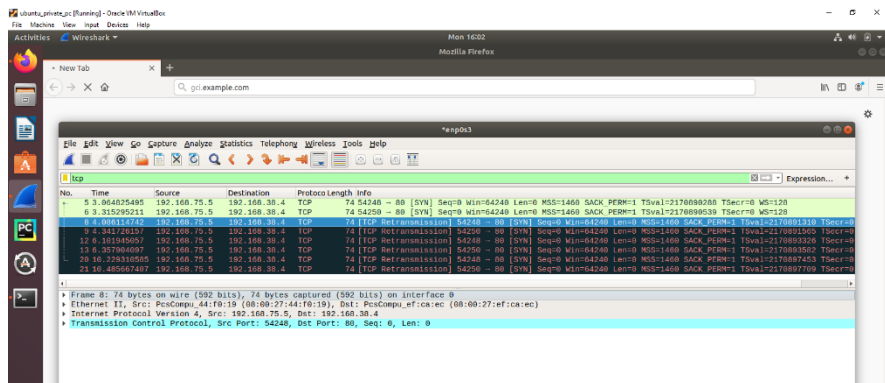
הסנפת התעבורה ממחשב ב-A לשרת האינטרנט על מחשב ב-D דרך שרת הפרוקסי על מחשב ב-B והסנפה על רשת B.

ניתן לראות את הפנייה ממחשב ברשת הפרטית (75.5...) לשרת הפרוקסי על רשת B (38.4...) על פורט 3128 שהוא הפורט המוגדר לשרת הפרוקסי על B. לאחר מכן ניתן לראות את החיבור בין שרת הפרוקסי לשרת האינטרנט על רשת D והעברת המידע ביניהם, ולבסוף העברת מרשת B אל דרך הפרוקסי.



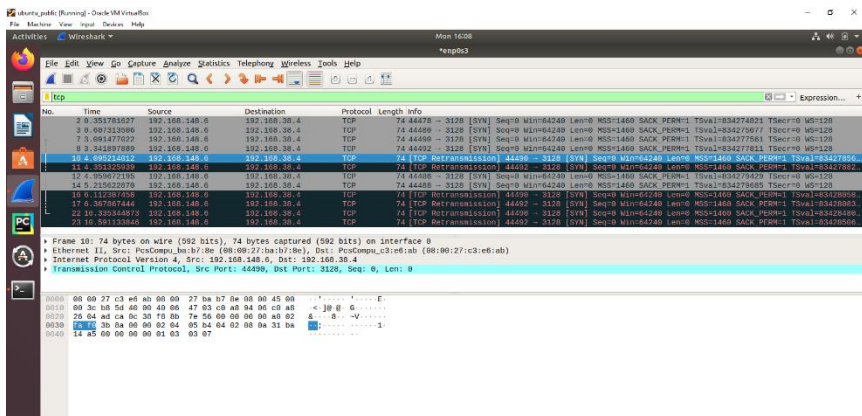
No.	Time	Source	Destination	Protocol	Length	Info
5.3	0.22933679	192.168.75.5	192.168.38.4	TCP	74	42916 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2175882525 TSecr=0 WS=128
6.8	0.22955273	192.168.38.4	192.168.75.5	TCP	74	3128 → 42916 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3399996699 TSecr=2
7.3	0.23773659	192.168.75.5	192.168.38.4	TCP	66	42916 → 3128 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2175882525 TSecr=3399996699
8.3	0.23879070	192.168.75.5	192.168.38.4	HTTP	440	GET http://gci.public.com/ HTTP/1.1
9.3	0.23911393	192.168.38.4	192.168.75.5	TCP	66	3128 → 42916 [ACK] Seq=1 Ack=381 Win=64896 Len=0 TSval=3399996699 TSecr=2175882525
10.3	0.24506961	192.168.38.4	192.168.148.6	TCP	74	36772 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=21454433493 TSecr=0 WS=128
11.3	0.25837423	192.168.148.6	192.168.38.4	TCP	74	80 → 36772 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=838812947 TSecr=1454..
12.3	0.25854592	192.168.38.4	192.168.148.6	TCP	66	36772 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=21454433493 TSecr=838812947
14.3	0.26217561	192.168.38.4	192.168.148.6	HTTP	500	GET / HTTP/1.1
15.3	0.26972545	192.168.148.6	192.168.38.4	TCP	66	80 → 36772 [ACK] Seq=1 Ack=435 Win=64768 Len=0 TSval=838812948 TSecr=21454433493
16.3	0.27011511	192.168.38.4	192.168.75.5	TCP	66	36772 → 42916 [ACK] Seq=1 Ack=381 Win=64896 Len=0 TSval=2175882525 TSecr=3399996699
17.3	0.27408987	192.168.38.4	192.168.148.6	TCP	66	36772 → 80 [ACK] Seq=435 Ack=430 Win=64128 Len=0 TSval=21454433496 TSecr=838812949
18.3	0.22459753	192.168.38.4	192.168.75.5	TCP	563	3128 → 42916 [PSH, ACK] Seq=1 Ack=381 Win=64896 Len=437 TSval=3399996789 TSecr=2175882525 [TCP se..
19.3	0.22631451	192.168.38.4	192.168.75.5	HTTP	160	HTTP/1.1 200 OK (text/html)
20.3	0.23296898	192.168.75.5	192.168.38.4	TCP	66	42916 → 3128 [ACK] Seq=381 Ack=438 Win=64128 Len=0 TSval=2175882624 TSecr=3399996789
21.3	0.23329351	192.168.75.5	192.168.38.4	TCP	66	42916 → 3128 [ACK] Seq=381 Ack=532 Win=64128 Len=0 TSval=2175882624 TSecr=3399996789
22.3	0.23389637	192.168.148.6	192.168.38.4	TCP	66	80 → 36772 [FIN, ACK] Seq=430 Ack=435 Win=64768 Len=0 TSval=838817953 TSecr=21454433496
23.3	0.23389637	192.168.148.6	192.168.38.4	TCP	66	36772 → 80 [FIN, ACK] Seq=435 Ack=431 Win=64128 Len=0 TSval=21454433500 TSecr=838817953
24.3	0.23389637	192.168.38.4	192.168.148.6	TCP	66	80 → 36772 [ACK] Seq=431 Ack=436 Win=64768 Len=0 TSval=838817953 TSecr=21454433500

לקוחות ברשת הפרטית לא יכולים לעקוף את הפרוקסי (באופן נאיבי). ניתן לראות בתמונה את ניסיון הפנייה לשרת האינטרנט ברשת B לאחר ששינית את הגדרות הדפדפן שלא להשתמש בפרוקסי. לא ניתן להתחבר לשרת האינטרנט על מחשב B, ובכלל לצאת מהרשת.



No.	Time	Source	Destination	Protocol	Length	Info
5.3	0.04032495	192.168.75.5	192.168.38.4	TCP	74	54248 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2176898288 TSecr=0 WS=128
6.3	0.31529511	192.168.75.5	192.168.38.4	TCP	74	54250 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2176898539 TSecr=0 WS=128
7.3	0.31529511	192.168.38.4	192.168.75.5	TCP	66	80 → 54250 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2176898539 TSecr=2176898539
8.3	0.34272857	192.168.75.5	192.168.38.4	TCP	74	[TCP Retransmission] 54250 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2176898539 TSecr=0
9.3	0.34272857	192.168.38.4	192.168.75.5	TCP	66	[TCP Retransmission] 80 → 54250 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2176898539 TSecr=2176898539
10.3	0.31545057	192.168.75.5	192.168.38.4	TCP	74	[TCP Retransmission] 54248 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2176898539 TSecr=0
11.3	0.31545057	192.168.75.5	192.168.38.4	TCP	74	[TCP Retransmission] 54250 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2176898539 TSecr=0
12.3	0.31545057	192.168.75.5	192.168.38.4	TCP	74	[TCP Retransmission] 54250 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2176898539 TSecr=0
13.3	0.31545057	192.168.75.5	192.168.38.4	TCP	74	[TCP Retransmission] 54248 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2176898539 TSecr=0
14.3	0.31545057	192.168.75.5	192.168.38.4	TCP	74	[TCP Retransmission] 54250 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2176898539 TSecr=0
15.3	0.31545057	192.168.75.5	192.168.38.4	TCP	74	[TCP Retransmission] 54250 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2176898539 TSecr=0

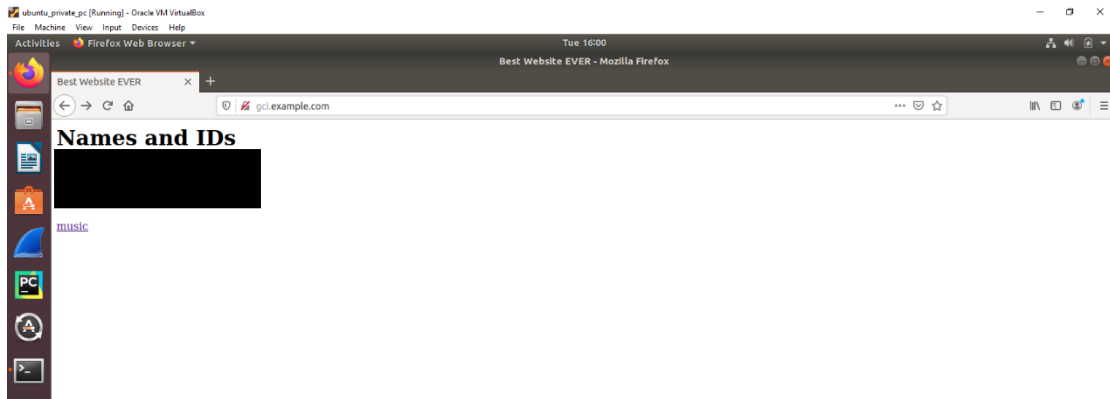
לקוחות ברשת D לא יכולים להקים חיבורים מול שרת הפרוקסי. ניתן לראות בתמונה את ניסיון הפנייה לשרת האינטרנט ברשת B לאחר ששינית את הגדרות הדפדפן ברשת D להשתמש בפרוקסי. לא ניתן להתחבר להקים חיבור כלל מול שרת הפרוקסי מרשת D החיצונית.



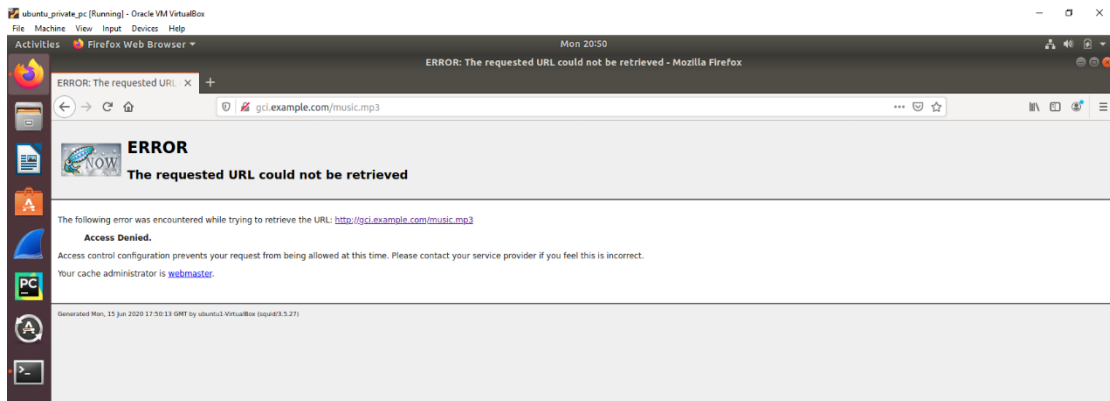
No.	Time	Source	Destination	Protocol	Length	Info
2.0	0.35176367	192.168.148.6	192.168.38.4	TCP	74	44476 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834278821 TSecr=0 WS=128
3.0	0.09731298	192.168.148.6	192.168.38.4	TCP	74	44480 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277577 TSecr=0 WS=128
4.0	0.09731298	192.168.148.6	192.168.38.4	TCP	74	44480 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277581 TSecr=0 WS=128
5.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0 WS=128
6.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
7.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
8.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
9.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
10.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
11.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
12.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
13.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
14.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
15.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
16.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
17.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
18.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
19.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0
20.0	0.34197989	192.168.148.6	192.168.38.4	TCP	74	[TCP Retransmission] 44492 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=834277811 TSecr=0

ה. הוספנו הגדרות ב squid.conf כך שיחסמו קבצי mp3 לפי regex.

לפני הלחיצה על הקישור:

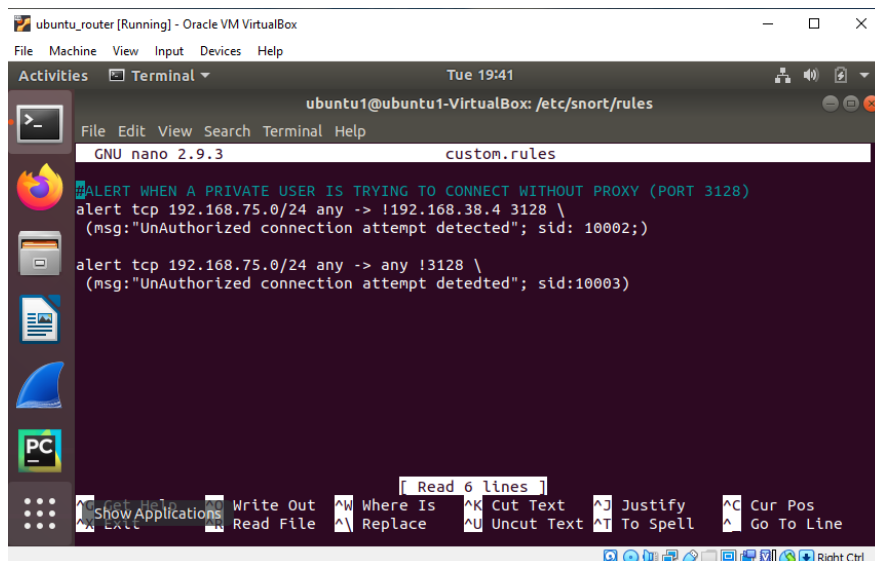


אחרי הלחיצה:



ו. הגדרנו את snort להאזין לכרטיס הרשת enps0s8 שמחובר לא. נכנסנו לקובץ הקונפיגורציה: /etc/snort/snort.conf ובו הגדרנו את כתובת home_net להיות 192.168.75.0, והוספנו rule חדש שייקרא מקובץ שיצרנו: /etc/snort/rules/custom.rules. הוספנו לקובץ זה 2 חוקים. החוק הראשון מורה לדווח על כל ניסיון תעבורת TCP שיוצאת מרשת A אל כל כתובת IP ששונה מכתובת הIP של שרת הפרוקסי. החוק השני מורה לדווח על כל ניסיון תעבורת TCP שיוצאת מרשת A אל כל PORT ששונה מכתובת הIP של שרת הפרוקסי. כך כיסינו את כל האופציות לניסיון תקשורת שלא מול הפרוקסי.

ניתן לראות את החוקים עצמם:



ניתן לראות שshort אכן מדווח כאשר יש ניסיון לגשת לקו או port ששונה משל הפרוקסי.

[illegible]

כדי לדווח על תקשורת מול הפרוקסי שמכילה פרטים אישיים בתוכנה, הוספנו עוד 4 חוקים לקובץ החוקים שלנו (חוק לכל שם ולכל ת"ז). החוקים מתריעים כאשר הם רואים content שזהה לפרטים האישיים שלנו, עם דגל nocase על השמות כדי שshortn יזהה גם מקרים שלא case sensitive. השתמשנו בfile_data לפני content כדי שshortn ידע לחפש בתוכן. החוקים:

The screenshot shows a terminal window titled "ubuntu_router [Running] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.9.3 text editor, editing the file "/etc/snort/rules/custom.rules". The user is "ubuntu1@ubuntu1-VirtualBox".

The content of the file is as follows:

```
#!ALERT WHEN A PRIVATE USER IS TRYING TO CONNECT WITHOUT PROXY (PORT 3128)
alert tcp 192.168.75.0/24 any -> !192.168.38.4 3128 \
(msg:"Unauthorized connection attempt detected"; sid:10002;)

alert tcp 192.168.75.0/24 any -> any !3128 \
(msg:"Unauthorized connection attempt detected"; sid:10003;)

#!ALERT PERSONAL INFORMATION
alert tcp 192.168.75.0/24 any <=> 192.168.38.4 3128 \
(msg:"Personal information detected"; file_data; content:"[REDACTED]"; nocase; sid:10004;)

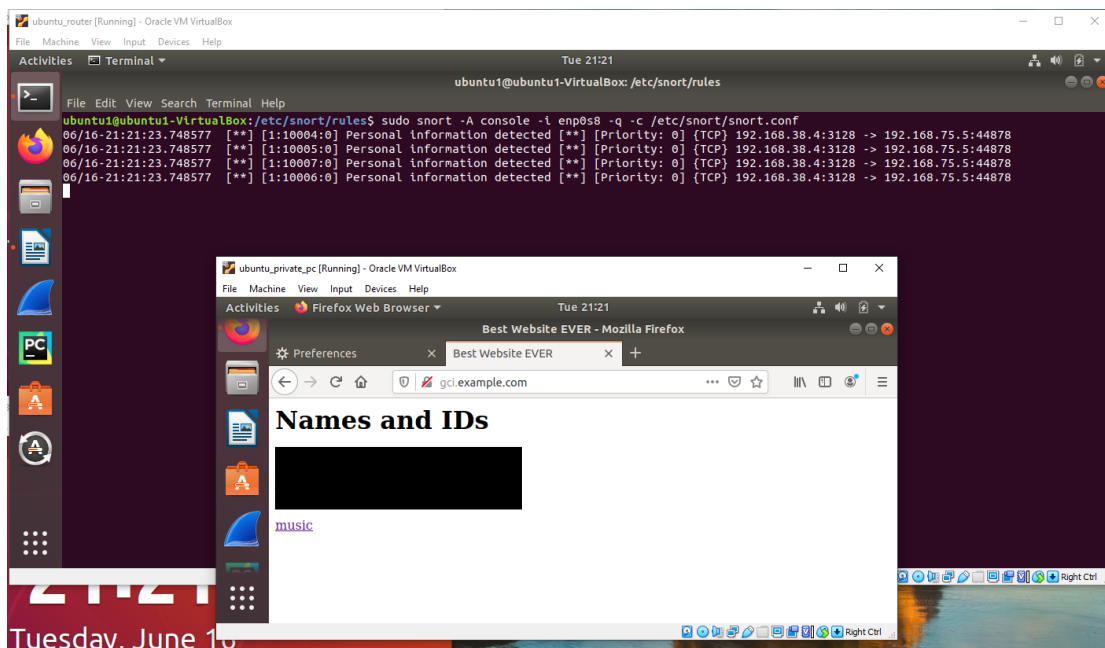
alert tcp 192.168.75.0/24 any <=> 192.168.38.4 3128 \
(msg:"Personal information detected"; file_data; content:"[REDACTED]"; nocase; sid:10005;)

alert tcp 192.168.75.0/24 any <=> 192.168.38.4 3128 \
(msg:"Personal information detected"; file_data; content:"[REDACTED]"; sid:10006;)

alert tcp 192.168.75.0/24 any <=> 192.168.38.4 3128 \
(msg:"Personal information detected"; file_data; content:"[REDACTED]"; sid:10007;)
```

A red rectangular box highlights the section starting with "#!ALERT PERSONAL INFORMATION" and ending with the last rule. The bottom of the terminal shows a status bar with various keyboard shortcuts and a prompt to "Read 19 lines".

ההתראות עצמן:



ז. כדי לאפשר סריקת nmap מ A לנשנה ספציפית לסעיף זה את טבלת iptables forward.
ובנוסף עדכנו את טבלאות הroute שלהם כדי שיכירו זה את זה.
בסעיף הקודם הגדרנו שכאשר מחשב מרשת A מנסה לשלוח מידע אל מחוץ לרשת שלא דרך הפרוקסי, snort ידווח על כך. לכן כיוון ששני המחשבים מכירים זה את זה (DI AM), ניתן לראות גם הודעות מסוג זה כיוון שהמחשבים בא יחזירו תשובה לבקשות של D.

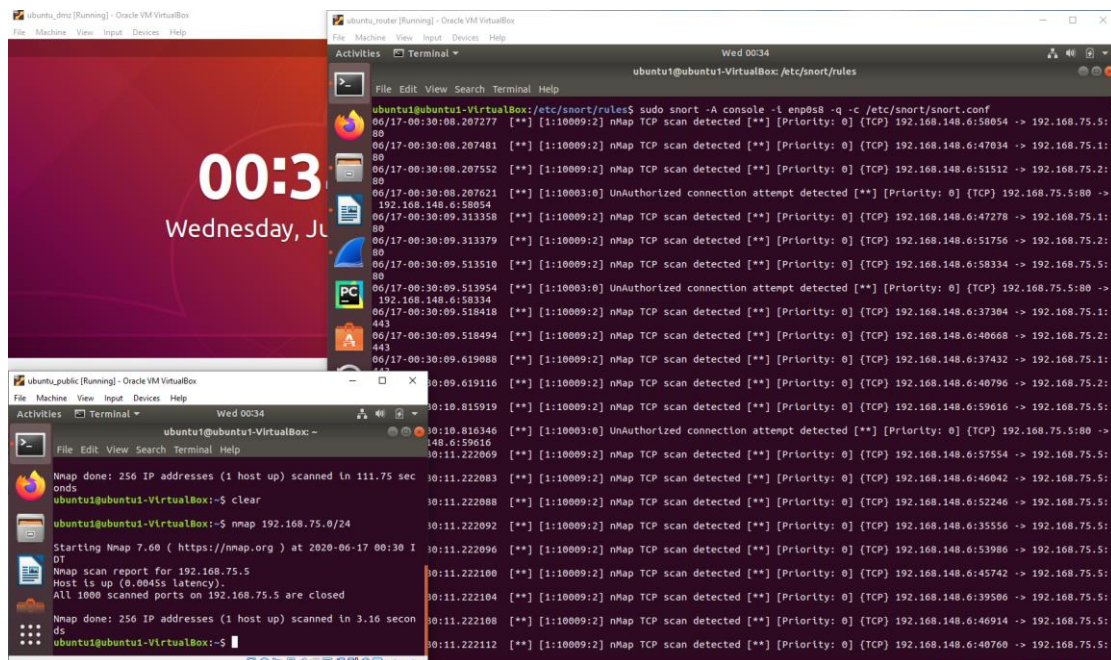
הוספנו את שלושת החוקים הללו לsnort על מנת שיזהה סריקת nmap:

```
#ALERT WHEN NMAP SCAN IS DETECTED
alert icmp any any -> 192.168.75.0/24 any \
(msg:"nMap PING sweep scan detected"; dsiz:0; sid:10008; rev:1;)

alert tcp any any -> 192.168.75.0/24 any \
(msg:"nMap TCP scan detected"; sid:10009; rev:2;)

alert udp !192.168.75.1 any -> 192.168.75.0/24 any \
(msg:"Nmap UDP scan detected"; sid:10010; rev:1;)
```

קעת בכל מצב, גם אם A לא תכיר את D, snort יזהה כל ניסיון סריקה בnmap בפרוטוקולים השונים.



ח. כדי להשתמש בsnort כIPS עלינו להשתמש בכללים אשר פועלים אקטיבית. עד כה השתמשנו בIDS, כלומר בכללים פסיביים שמתריעים לנו למשל כאשר כתובת IP מסוימת סורקת או מתקיפה אותנו. IPS, בשונה מIDS, פועל אקטיבית כנגד החבילות החשודות. נוכל להגדיר כללים כמו: drop (חוסם ושומר לוג של החבילה), reject (חוסם ושומר לוג של החבילה, ובנוסף גם שולח TCP reset או הפרוטוקול היה TCP או ICMP port unreachable) או UDP (sdrops, (חוסם את החבילה אך לא שומר לוג). באמצעות חוקים אלו נוכל לחסום אקטיבית בזמן אמת חבילות חשודות ונוכל במידת הצורך לחסום את כתובת הIP ששלחה לנו את החבילות החשודות, או לטפל בכל דרך שנבחר. חוק לדוגמא:

Reject tcp any any <> 192.168.75.0/24 any \

(msg:"Dropped malicious traffic from www.evil.com"; content:"evil.com"; nocase; sid:10000;)

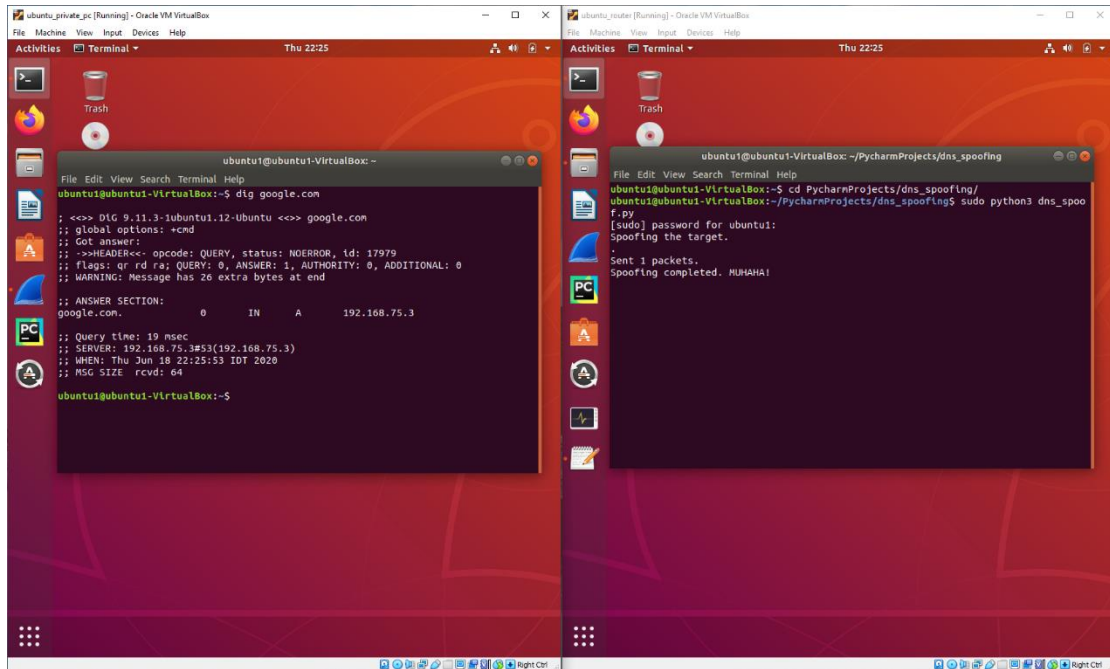
חוק זה יחסום את האתר הנ"ל בכל מחשבי הרשת הפרטית (A), ידווח ללוג וישלח הודעת TCP reset.

ט. הסבר של הסקריפט: הסקריפט מרחרחר אחר חבילות מפרוטוקול UDP עם פורט 53 (DNS) מרשת A. במידה ומגיעה אל הראוטר חבילה שעונה על הדרישות, הסקריפט יבדוק האם היא בקשת DNS. במידה וכן, הוא יבדוק האם הדומיין google.com נמצא בתוך הבקשה. במידה וכן הוא אנו יוצרים באמצעות scapy:

- חבילת IP ובו אנו בעצם הפכים את המקור והיעד של החבילה המקורית, כך שיראה שהחבילה הגיעה מהמקום הנכון.
- חבילת UDP כך שפורט המקור שלה הוא 53 (DNS) והיעד הוא המקור של החבילה המקורית.
- חבילת DNS עם id של החבילה המקורית, והדגלים הנכונים לתשובת DNS.
- חבילת DNSRR ובה שם הדומיין עליו הבקשה שאלה, והIP המזויף שלנו rdata.

אנו מאחדים הכל לחבילה אחת ושולחים אותה בחזרה לא.

ניתן לראות את בקשת dig מ (משמאל) google.com ואתה קוד הפייטון שלנו מורץ בראוטר (ימין).



ניתן לראות ב-Wireshark א2 שנשלחה שאילתת DNS וחזרה תשובת DNS תקינה עם כתובת IP מזויפת.

