

אוניברסיטת אריאל

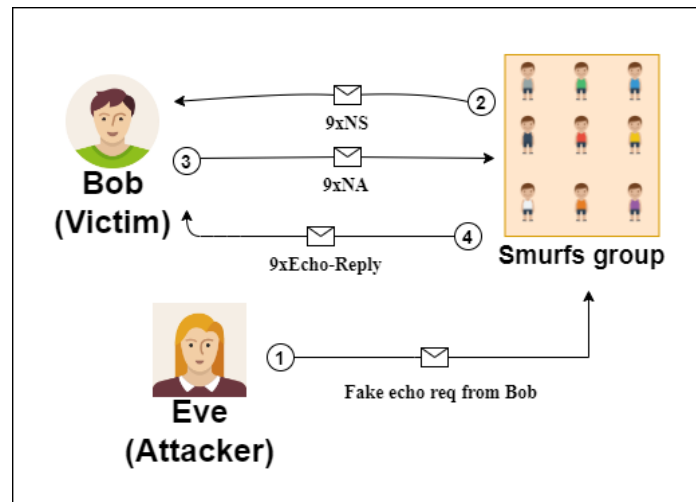
הגנת פרוטוקולי תקשורת

סמסטר אביב

SMURF ATTACK

שמות מגישים: עמית גופר, שמחה טייך, אמיר ג'ילט

ראשית, אנו נסקור בקצרה את הליך המתקפה ע"י דיאגרמה:



עתה, מאחר שיש לנו 4 מכונות, אזי קב' ה-"דרדרסים" שלנו תהיה 2 מכונות, ועוד 2 מכונות בצד - האחד לתוקף והשני לנתקף. הואיל וכעת איננו מצליחים לקנפג כתובת *multicast* עבור קב' מכונות ספציפית, אנו נשתמש בכתובת *multicast* שכל *node* מחזיק שהיא: `ff02::1`, ומפני שהתוקף מבצע את ה-*spoofing* מהנתקף (Bob), לכן, הן התוקף והן הנתקף מפילים את הפקטה של הבקשה. מכאן, שנוכל לדמות את השליחה לקב' ע"י שליחה לכתובת הנ"ל.

לפני שנסביר על השלבים, נסקור את התת רשת בטבלה קצרצרה:

-	<i>Victim – Bob</i>	<i>Attacker – Eve</i>	<i>nodes (smurf group)</i>
IP	<code>fe80::487c:ed58:ca1c:3dd8</code>	<code>fe80::43b5:d6fa:8613:4d7e</code>	<code>ff02::1</code>

נסביר מעט על השלבים שמוצגים בדיאגרמה הנ"ל.

שלב ראשון - spoofing: התוקף (במקרה זה איב), שולח פקטה מזוייפת - כאשר מקורה (*source*) היא הכתובת הפרטית של הנתקף (היינו - בוב) וכי יעדה (*destination*) היא קב' הדרדרסים. הפקטה נבנתה תחת *scapy* בקוד שאותו אנו מריצים ששולח ובונה את אותה פקטה עם אותם פרטים רלוונטים של תת הרשת. קובץ הקוד נקרא *spoofing.py*, ואנו נריץ אותו מהטרמינל עם *sudo*. בנוסף לצורך ההמחשה, אנו שלחנו 10 בקשות *echo – request* לקב' הדרדרסים, ולכן אנו מצפים בהתאם ל-20 תגובות (גודל קב' הדרדרסים 10). יתרה מזאת, נקליט מהנתקף את כל התקשורת (נפלטת עם *icmpv6*) במהלך התקיפה כדי להוכיח שבאמת כל השלבים קרו.

שליחת הפקטה המזוייפת (נעשה את זה לאחר ניקוי ה-*cache* אצל קב' הדרדרסים, כדי שנראה בהתאם את השלבים בדיאגרמה, שכן אחרת לא נראה באותו סדר את ה-NA ו-NS - ניתן לראות הסבר לניקוי זכרון המטמון בשלב השני ושלישי):

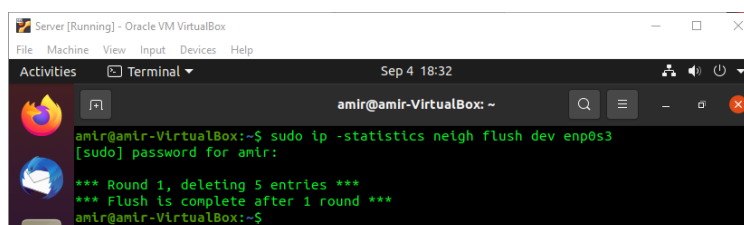
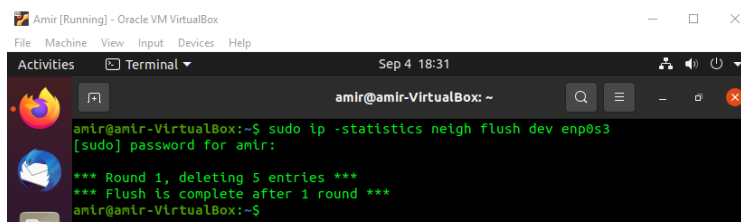


שלב שני ושלישי: ננקה את ה-cache במחשבי קב' הדרדרסים, על מנת לראות את שתי פקטות NS שנשלחות ע"י קב' הדרדרסים ואת שתי פקטות NA שהנתקף - בוב משיב.

לשם ניקוי ה-cache נעזר בפקודה הבאה.

```
sudo ip -statistics neigh flush dev enp0s3
```

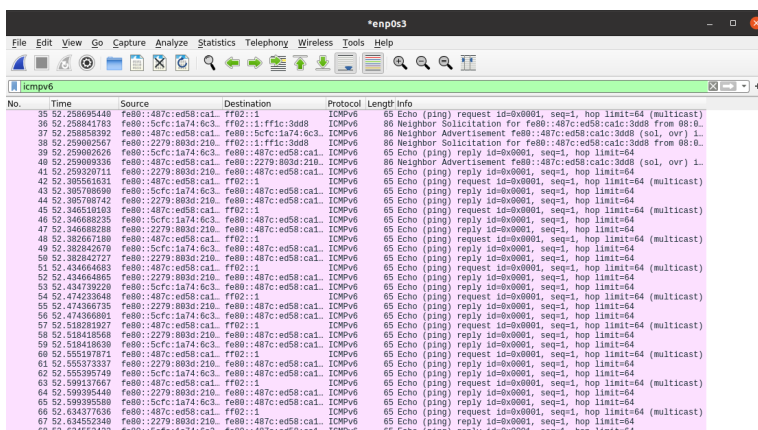
נכתוב זאת בכל אחד ממחשבי קב' הדרדרסים.



• הערה: את הניקוי נעשה לפני שליחת הפקטה בשלב הראשון.

שלב רביעי ואחרון: שליחת תגובה (echo – reply) מכל אחד בקב' הדרדרסים.

נראה שבהקלטת ה-*Wireshark* (אצל הנתקף) את כל השלבים של הדיאגרמה.

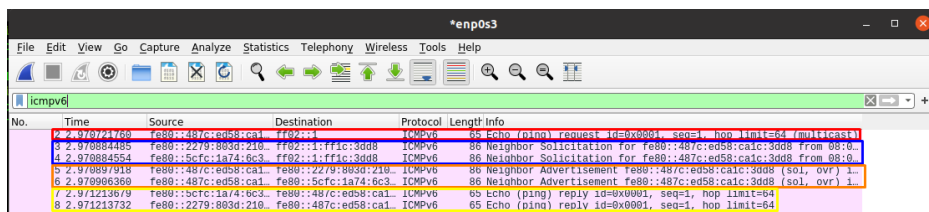


No.	Time	Source	Destination	Protocol	Length	Info
35	52.258695448	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
36	52.258841783	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
37	52.258858392	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
38	52.259002567	fe80::2279:803d:210c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
39	52.259002026	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
40	52.259009336	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
41	52.259120711	fe80::2279:803d:210c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
42	52.259120531	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
43	52.259120531	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
44	52.259120742	fe80::2279:803d:210c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
45	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
46	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
47	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
48	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
49	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
50	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
51	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
52	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
53	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
54	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
55	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
56	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
57	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
58	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
59	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
60	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
61	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
62	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
63	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
64	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
65	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
66	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
67	52.259120742	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
68	52.259120742	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)

ניתן לראות כי בסך הכל ישנם 20 תגובות - כפי הנדרש. בנוסף, ניתן לראות את שלב ראשון בפקטה הראשונה כן בהקלטה לאחר פלטור, מיד לאחר מכן ניתן לראות שכל אחד מקב' הדרדרסים שלח NS וקיבל תגובה NA מן הנתקף, ולאחר מכן הנתקף השיב ב-*echo – reply*.

- אם הייתה בקשה אחת שנשלחת היינו רואים את זה יותר ברור. לכן, נעשה זאת ונשלח בקשה אחת.

נשלח בקשה אחת במקום 10.



No.	Time	Source	Destination	Protocol	Length	Info
2	2.970974769	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
3	2.970984485	fe80::2279:803d:210c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
4	2.970984454	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
5	2.9709897918	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
6	2.9709908369	fe80::487c:ed58:ca1c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)
7	2.971213679	fe80::5cfc:1a74:6c3c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (multicast)
8	2.971213732	fe80::2279:803d:210c::ff02::1	ff02::1	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (multicast)

- **באדום - שלב ראשון:** בקשת *echo – reply* אשר כביכול נעשית מהנתקף.
- **בכחול - שלב שני:** שתי בקשות NS מצד הדרדרסים.
- **בכתום - שלב שלישי:** שתי תגובות NA מצד הנתקף.
- **בצהוב - שלה רביעי ואחרון:** 2 תגובות *echo – reply* מצד הדרדרסים.

בדיוק כפי שציירנו בדיאגרמה!