טכנו"צ סייבר – תרגיל 4 - "SPOOF"

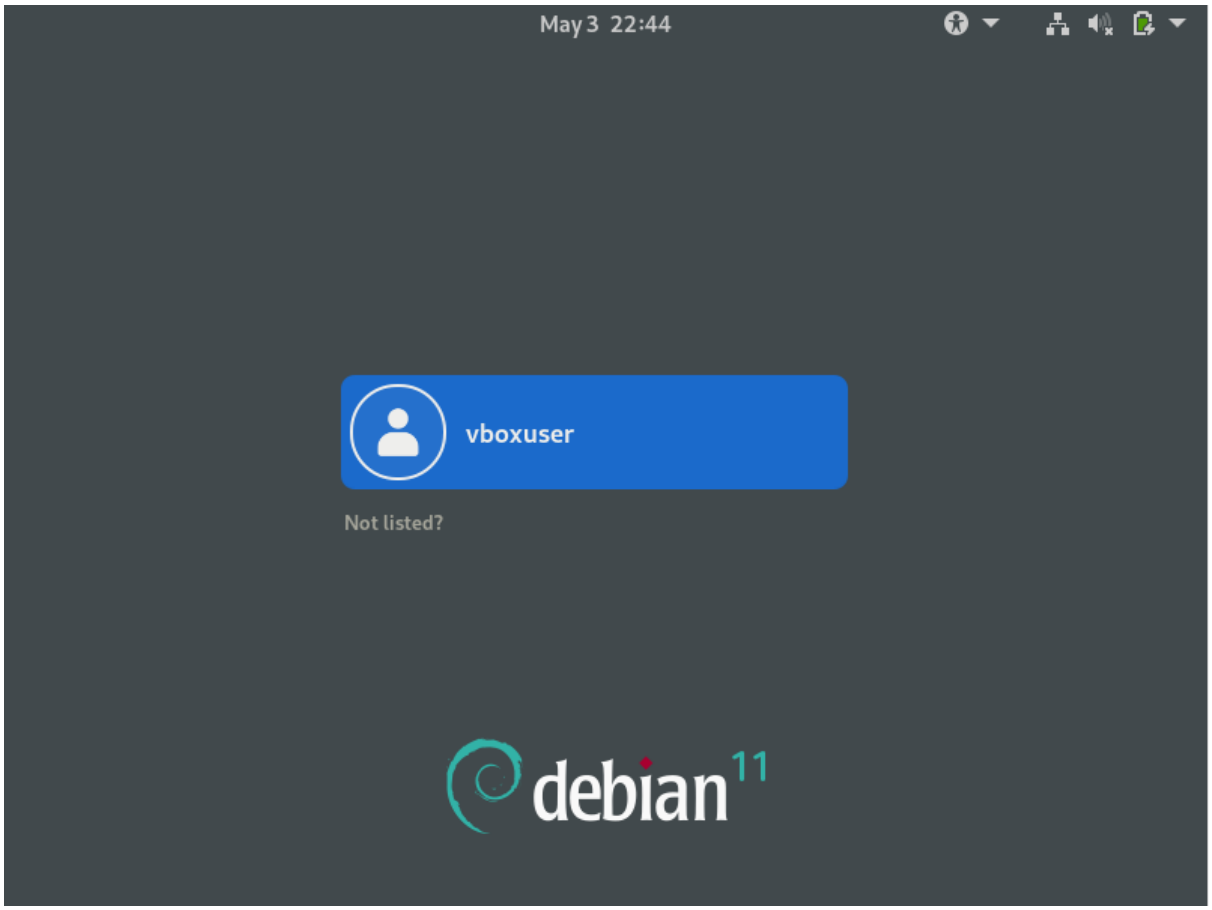
שימוש במכונה וירטואלית לבדיקת התרגיל

מטרת העל

בניגוד לתרגילים קודמים, תרגיל 4 כולל תקשורת בין מספר נקודות קצה שונות, ולכן מחייב שימוש ברשת אינטרנטית בצורה כלשהי. הדרך הסטרילית ביותר לבדוק את התרגיל (נדגיש ש**אין חובה** לבדוק אותו ככה) היא בעזרת שתי מכונות וירטואליות, תוקף ונתקף, שרצות מעל המחשב שלכם בו זמנית ומקיימות את הרשת.

בניית הסביבה

בקישור הבא תמצאו קובץ מסוג **ova.** שהוא מכונה וירטואלית מוכנה ארוזה לשימושכם. מכונה זו מכילה את כל מה שצריך על מנת להריץ את התרגיל. לידע כללי זו מכונה שמריצה מערכת הפעלה מסוג **Debian**, שזו הפצה מוצלחת של לינוקס שנבחרה לבדיקה כאיזון בין שימושיות לבין זה שהיא לא כבדה מדי (בג'יגה-בייט).
על מנת לארגן את סביבת הבדיקה, הורידו את הקובץ ופתחו אותו בעזרת **VirtualBox**. לחצו **finish** על מנת לבנות מכונה וירטואלית מקובץ ה **ova.** וחכו עד לסיום הבנייה.
ודאו שהכל בסדר – הריצו את המכונה הוירטואלית.



הגעתם למסך כזה? מצוין! זה מסך ההתחברות. **vboxuser** הוא שם המשתמש שלם והסיסמא היא **changeme**.

טכנו"צ סייבר – תרגיל 4 - **"SPOOF"**

אם זה מה שנגלה לעיניכם לאחר הזנת הסיסמא, הכל מצוין. כבו את המכונה הוירטואלית ונחזור לעבוד.
על מנת ששתי המכונות שלכם יוכלו לתקוף זו את זו, **VirtualBox** צריכה לחבר את המכונות הוירטואליות שאתם יוצרים לרשת אחודה (על פני רשת ממודרת לכל מכונה וירטואלית). ודאו שהמכונה היחידה שיש לכם בינתיים מוגדרת כך על פי המדריך הזה (תחת הכותרת **How to Network Two Virtual Machines Using Virtual Box**).
כעת כמובן, צריך שניים לטנגו – וגם צריך שתיים לתקיפת סייבר מוצלחת. לחצו מקש ימני על השורה של המכונה הוירטואלית שלכם בתפריט של **VirtualBox** ובחרו באפשרות **clone**. תנו שם למכונה החדשה ובחרו תחת **MAC Address Policy** את האפשרות **Generate new MAC addresses for all network adapters**. לחצו **Next** ושימו לב שאתם בוחרים **Full clone** לפני שאתם לוחצים **Finish**. שימו לב שלאחר השלמת פעולה זו אמורות להיות לכם שתי מכונות נפרדות על המחשב ומבחינת **VirtualBox**, שהן זהות מכל בחינה. אחת מהן תהיה מחשב התקיפה שלנו (מכונת התוקף), והאחרת תהיה הנתקף האומלל (מכונת הנתקף).
הרימו את שתי המכונות במקביל, בדקו את הכתובות שלהן וודאו שהן נגישות ב-**ping** אחת לשנייה (פקודות רלוונטיות בעמוד האחרון של מדריך זה).

טכנו"צ סייבר – תרגיל 4 - **"SPOOF"**

הכירו את סביבתכם הקרובה

כעת הדליקו את אחת המכונות.

מצד שמאל למעלה ניתן לשים לב למילה **Activities**, שהיא מעין 0פריט ההתחלה של **Debian**.

בלחיצה עליה מופיעה שורת חיפוש. אתם אמורים להצטרך במהלך התרגיל שלוש אפליקציות בערך:

- **Files**, סייר הקבצים
- **Firefox**, דפדפן
- **Terminal**, שזה כמו **cmd**

על מנת להעביר קבצים לתוך המכונה מומלץ להשתמש ב **Firefox**, ולהעביר את הקבצים דרך **Google Drive** או תוכנת שיתוף קבצים אחרת.

הגדרות רשת על המכונות הוירטואליות

- עלול להיות קצת קשה להבין מה שרת ה-**DNS** המקומי במקרה זה[1]. בהגדרות של קובץ הקוד שלכם, קחו את ה-**IP** שלו להיות **10.0.2.43**.
- שרת ה-**DNS** החיצוני שאתם משתמשים בו כדי לטפל בבקשות אמיתיות יכול להיות **8.8.8.8** או כל שרת לגיטימי אחר שתרצו.
- את ה-**IP** של התוקף והנתקף אתם יכולים להבין בצורה דומה לצורה שבה זה נעשה על המחשבים של עצמכם – ראו פקודות רלוונטיות בהמשך.
- אם ה-**IP** של התוקף והנתקף לא נמצאים בתת הרשת של **10.0.2.43**, אולי כדאי לקרוא את ה-**footnote** פה למטה ולשנות את **/etc/resolv.conf** בהתאם. שימו לב שצריך הרשאות אדמין לכך (תריצו **sudo nano /etc/resolv.conf**).
- חשוב: **בכל פעם** שאתם מדליקים/עושים **restart** למכונת הנתקף, פתחו בה **Terminal** והריצו את הפקודה **./update_resolv_conf.sh** (כולל הנקודה והסלאש). זה סקריפט שיבקש מכם הרשאות **sudo** ויגדיר את שרתי ה-**DNS** שהנתקף מכיר כדי שהכל ינגן.

הסבר קצר על לינוקס

[1] הקובץ /etc/resolv.conf מכיל רשימה של IP-ים של שרתי DNS ושליחת שאילתות DNS היא לשרתים הנ"ל לפי הסדר. במכונה שקיבלתם מוגדר שם ה-IP שכתוב למעלה ואחריו שרת לגיטימי (8.8.8.8). ההנחה היא ששרת שזה ה-IP שלו לא קיים ברשת של המחשב שלכם עם שתי המכונות ולכן המכונה תעשה fallback לשרת הלגיטימי תחת התהגות נורמלית. במידה ויש גורם זדוני במערכת שטוען שהוא 10.0.2.43 (אהמ) מערכת ההפעלה תפנה אליו קודם ולכן הוא ידרוס את השרת הלגיטימי. כך במובן מסוים אנו מחקים התנהגות של תגובה ל-arp spoofing במערכת עם שרת DNS מקומי אמיתי (רק ללא התחרות עם השרת האמיתי).

טכנו"צ סייבר – תרגיל 4 - **"SPOOF"**

Debian היא הפצה של **Linux** ולכן רוב הכללים שאתם אולי מכירים על לינוקס חלים עליה. כשאתם מחפשים בגוגל איך לעשות משהו, שווה להוסיף את המילה **Debian** (ולא **Linux**) בשורת החיפוש כדי לקבל תוצאות רלוונטיות ל-**Debian** ספציפית, יש הבדלים קלים בין ההפצות.

פקודות רלוונטיות:

sudo מאפשרת להריץ פקודות בהרשאה גבוהה – כל פקודה שעושה לכם בעיות תריצו שוב עם **sudo** לפני. למשל **wireshark** לא תצליח להסניף אם תריצו אותה ככה סתם אז תריצו **sudo wireshark**.

- **nano** הוא עורך טקסט חביב שיכול להיות נוח לעריכת קבצים אם אתם כבר בטרמינל. שימוש: **nano <path to file>**.
- **ip addr** ו-**ip neighbor** נותנות לכם מידע על נתוני הרשת של עצמכם ושל המחשבים השכנים ברשת, בהתאמה.
- **curl** מאפשר לפנות לאתר אינטרנט מהטרמינל ללא דפדפן, יכול להיות נוח לדיבאגינג.
- **wireshark** יפתח לכם את תוכנת ההסנפה המוכרת והאהובה.
- **python3, pip** כמו שאתם מכירים ואוהבים (שימו לב ל-3). הספריות שאתם צריכים אמורות להיות מותקנות כבר, אבל אם יש צורך בעוד – תתקינו עם **sudo** (**sudo pip install <lib>**).

בהצלחה!