



פתרון מעבדה 1



התקפת תקשורת DoS DDoS

Apache DoS Lab

- עמוד 1 -

כל הזכויות שמורות © סיבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383



הבנת הדרך לביצוע התקפת DoS באמצעות Kali Linux נגד Apache.



30-45 דקות

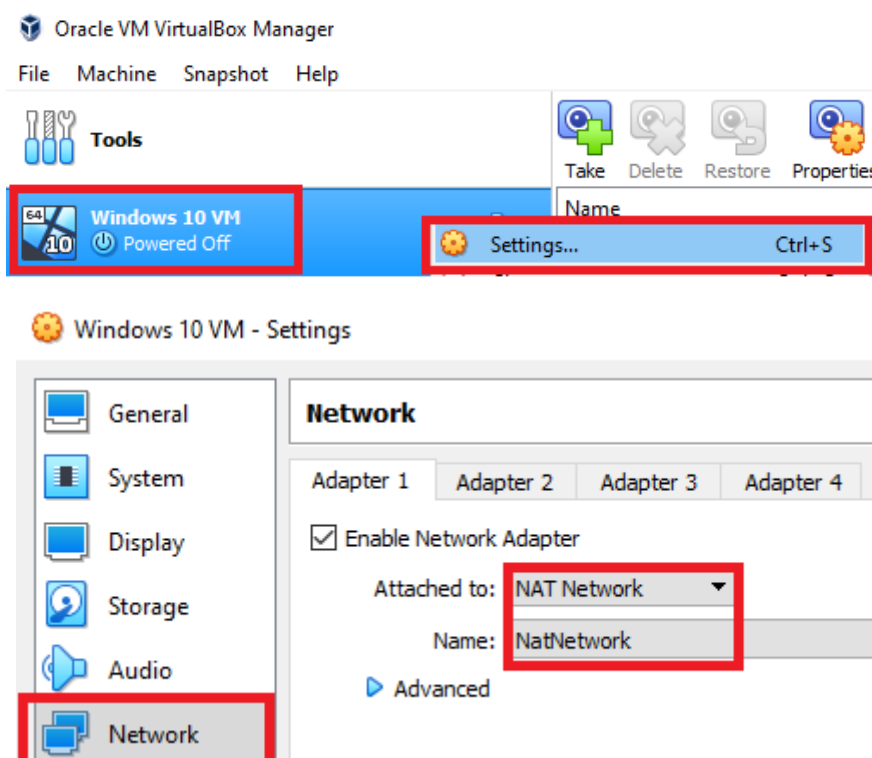


- VirtualBox <
- Kali Linux <
- Windows 10 <
- XAMPP (מסופק בקבצים נוספים) <

יש להתקין את Apache ב-Windows

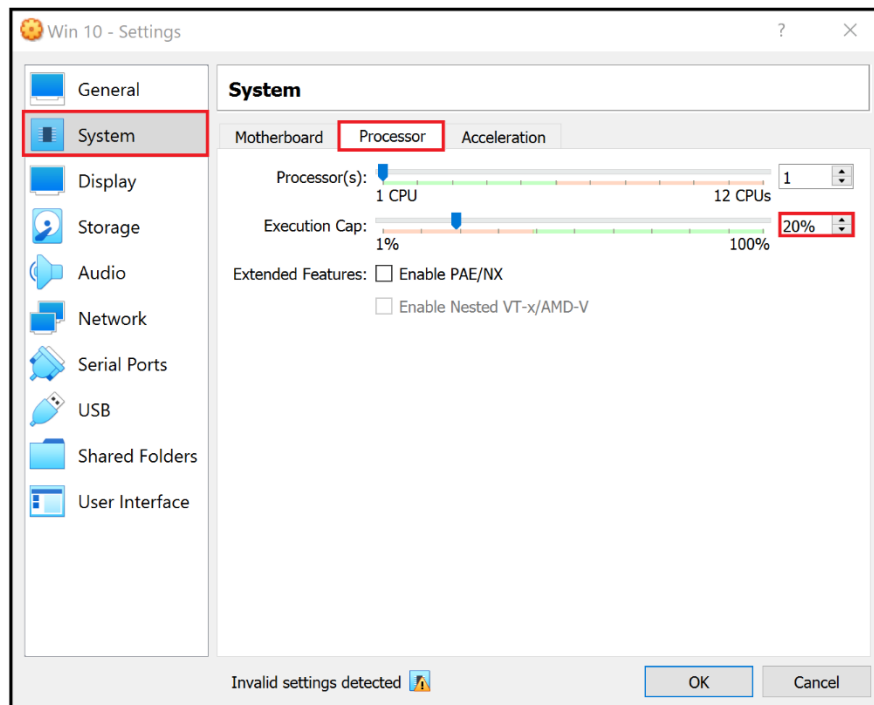
יש להתקין את XAMPP ב-מכונה הווירטואלית Windows 10 VM.

- 1 ב-Oracle VM VirtualBox Manager, יש ללחוץ קליק ימני על שם המכונה ולבחור באפשרות **Settings...** יש לנווט למקטע **Network** ולוודא ששני המחשבים מוגדרים אל אותה רשת NAT.
הערה: יש לבצע את השלב הזה במכונה הווירטואלית של Kali Linux ושל Windows 10.

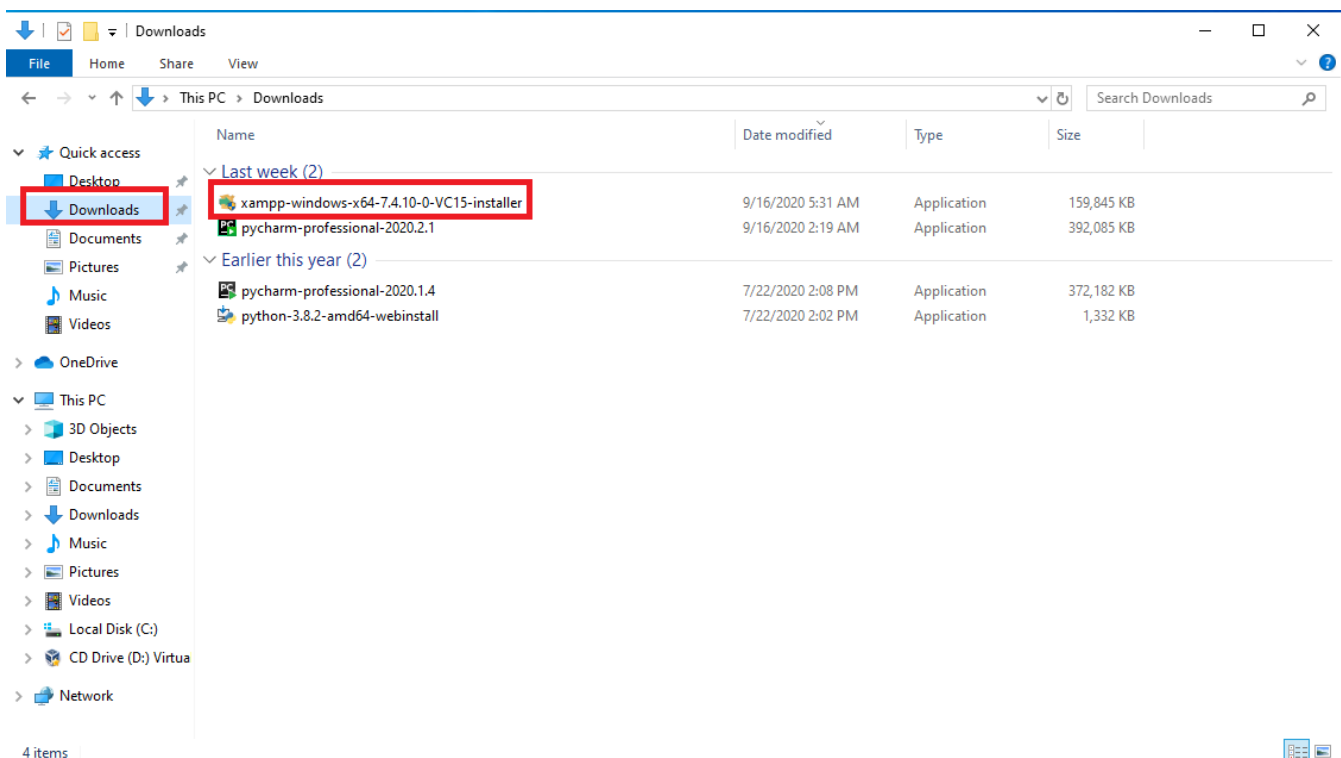


- 2 יש להישאר ב-**Settings** בתוך המכונה של Windows 10, ללחוץ על הלשונית **System** ולעבור אל הלשונית **Processor** כדי להקטין את ה-**Execution Cap** (מבסת ביצוע) ל-20% ולאחר מכן ללחוץ על **OK**.

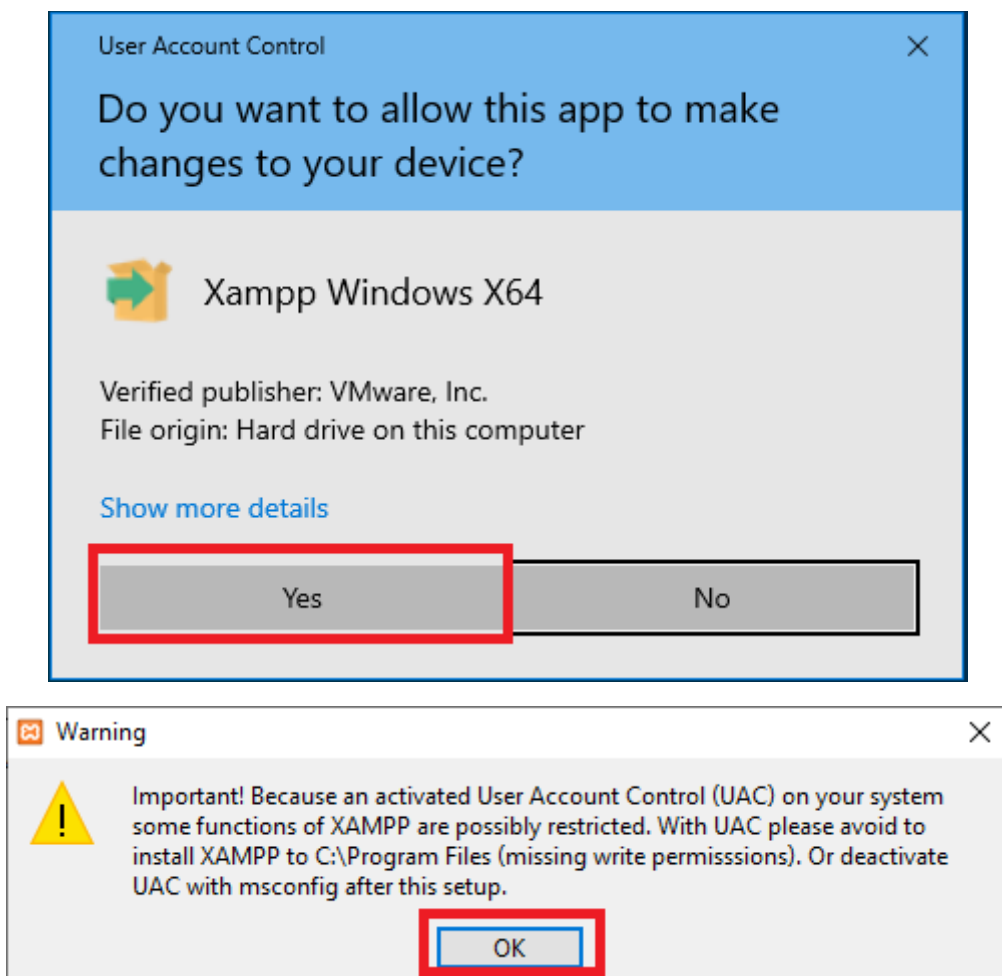
הערה: ניתן להתאים את מבסה הביצוע מכיוון שהמכונה הווירטואלית חיה כדי להשיג את התוצאות הנכונות.



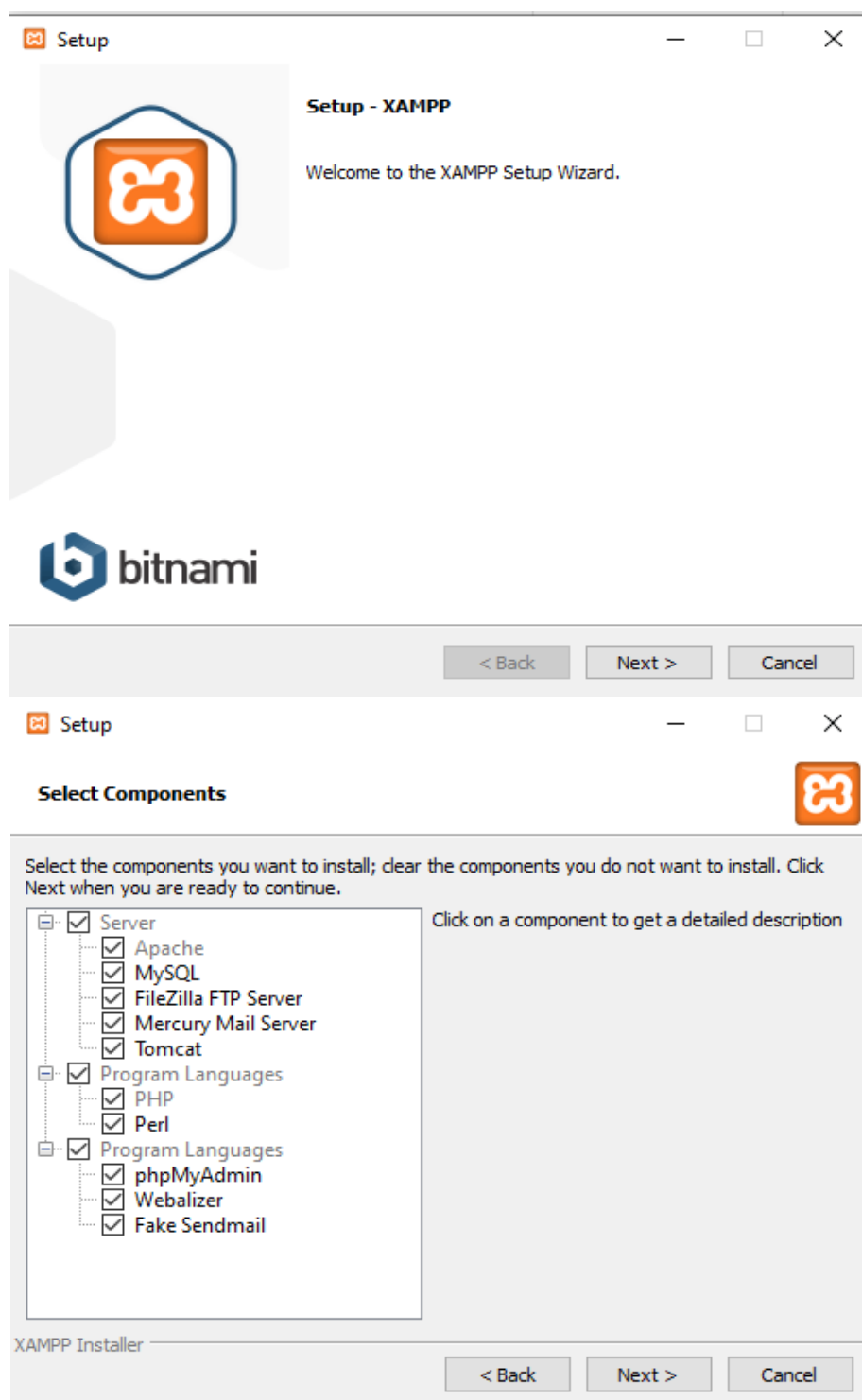
3 XAMPP מסופק על ידי המנחה. יש להעתיק את קובץ ההפעלה אל VM Windows 10 וללחוץ לחיצה בפולה על הקובץ כדי להתחיל בהתקנה.

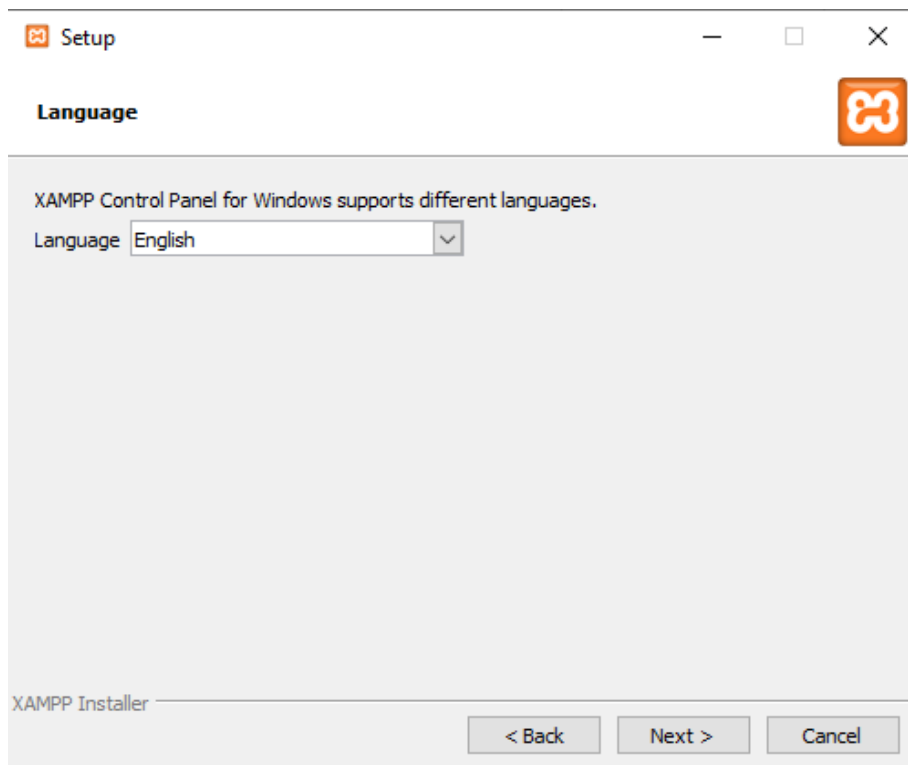
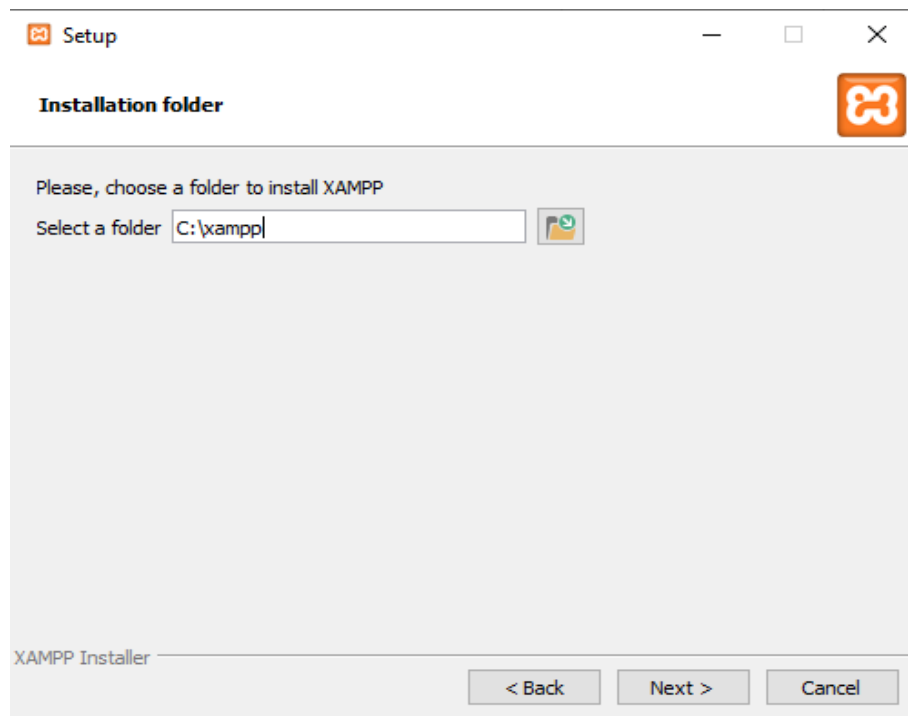


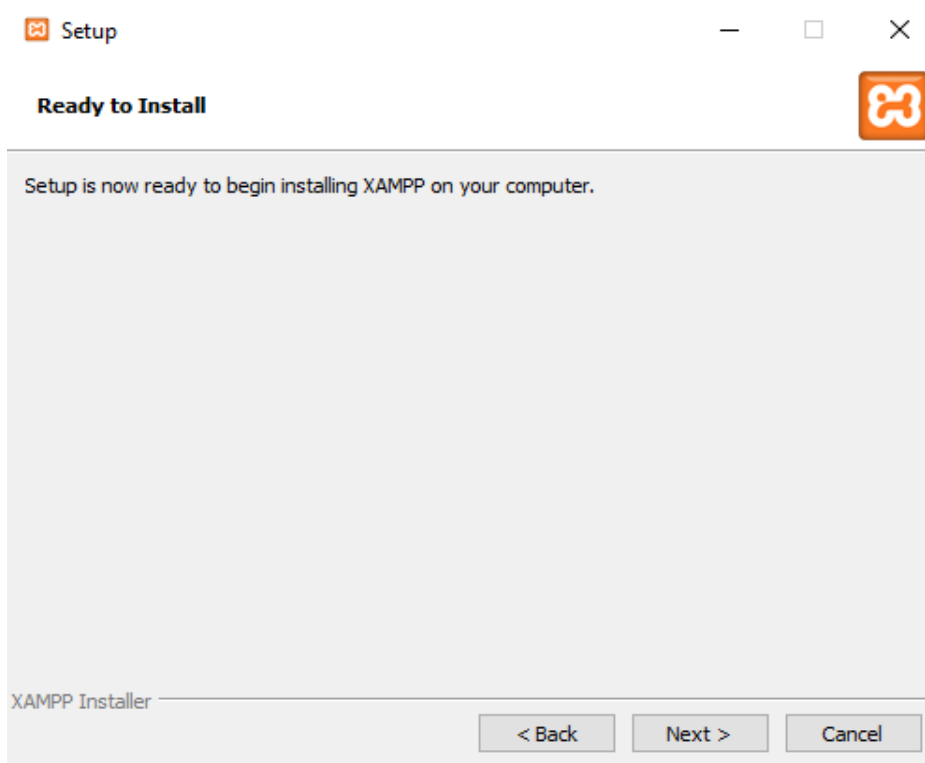
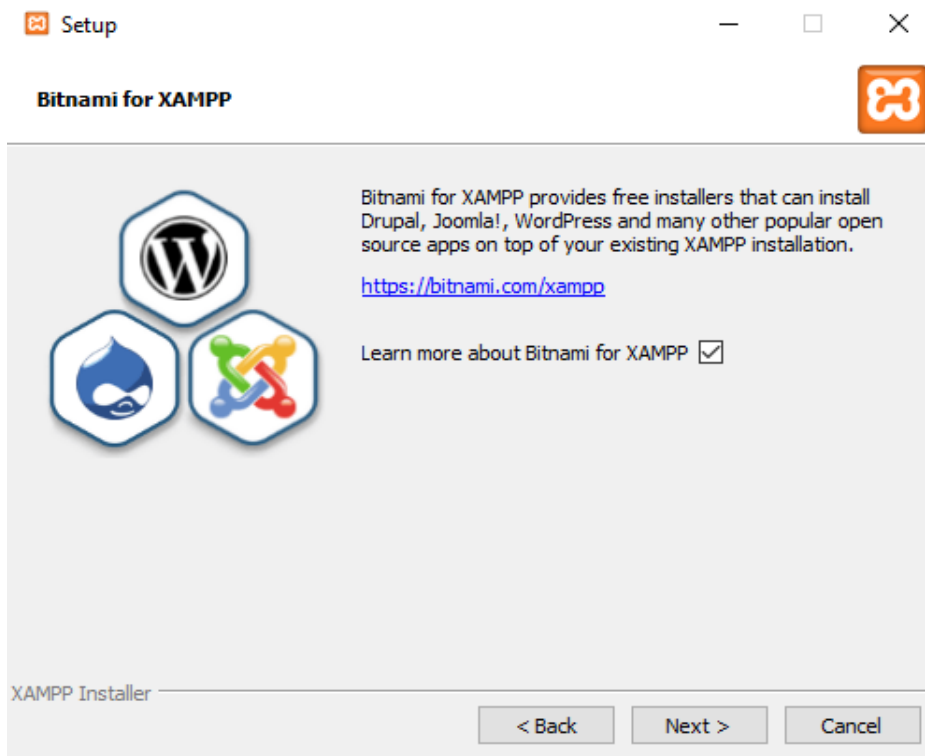
4 יש ללחוץ על **Yes** בחלון User Access Control (בקרת גישה משתמש). יש ללחוץ על **OK** בתיבת האזהרה.



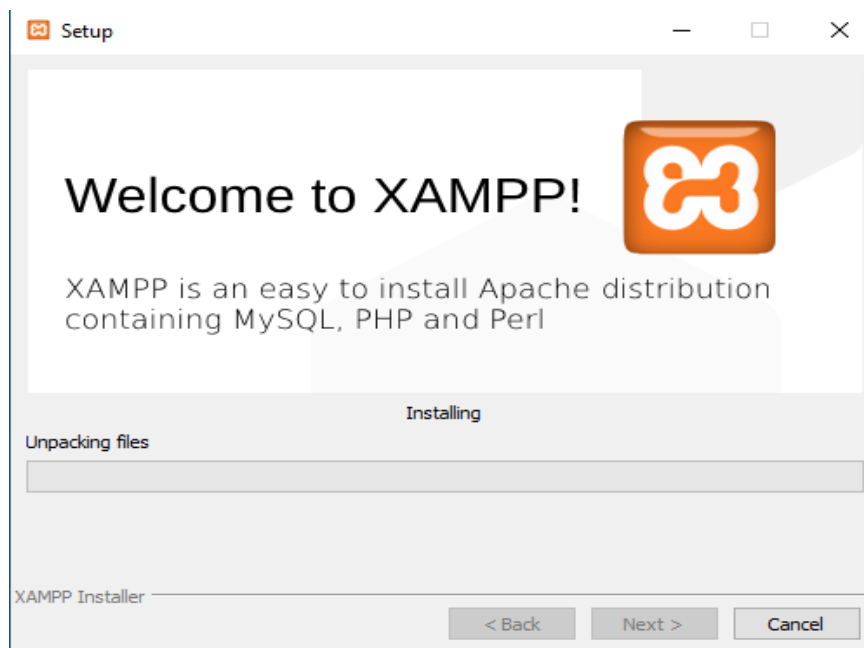
בתוך תוכנית ההתקנה של XAMPP, יש ללחוץ על **Next** בכל חלונות ההתקנה.



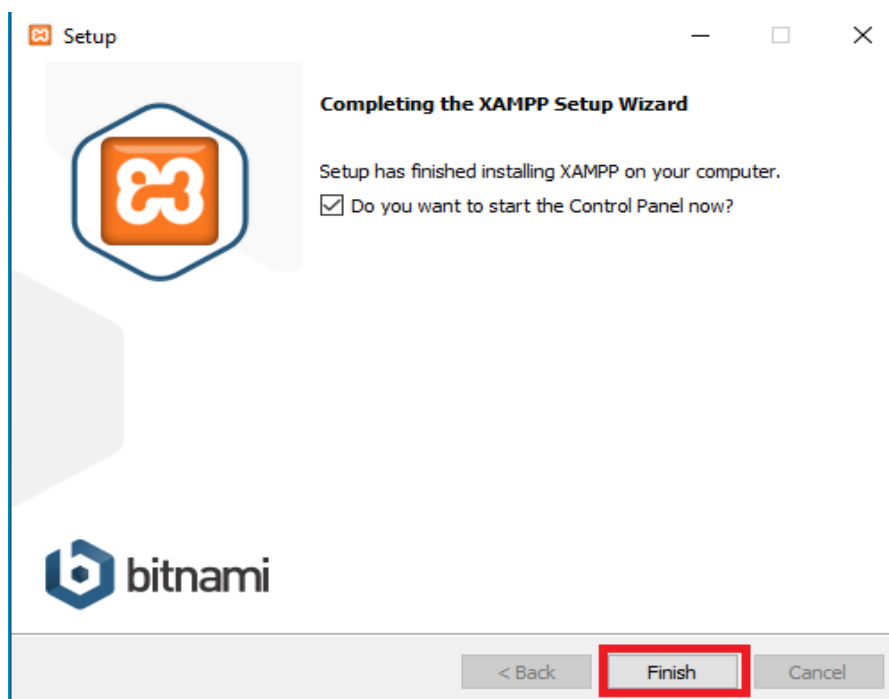




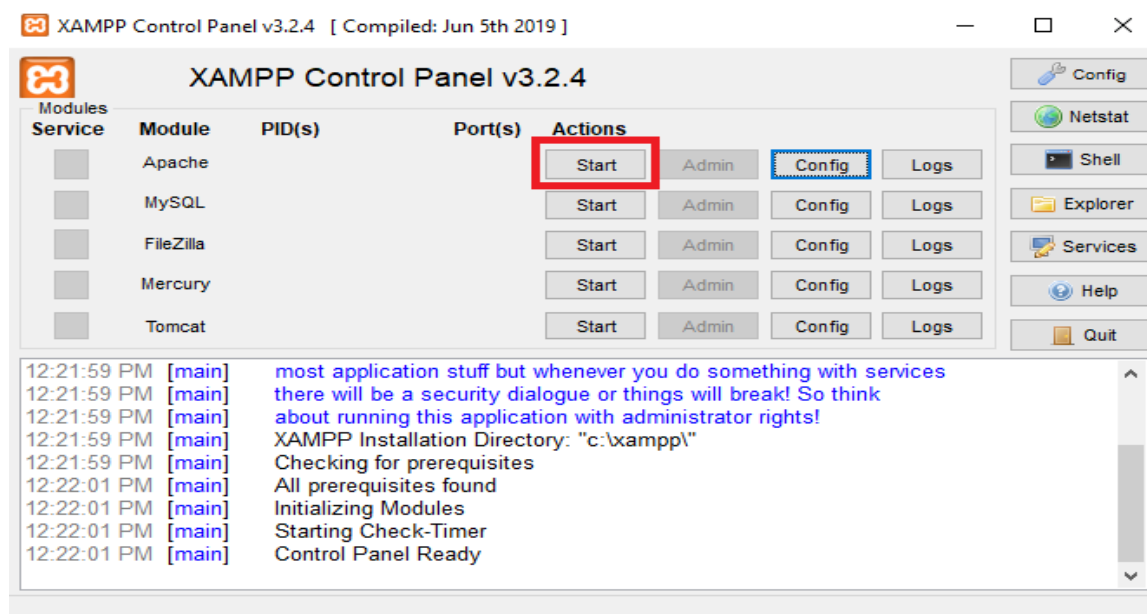
6 ההתקנה תמשיך להתקין את הקבצים הדרושים להפעלת Apache.



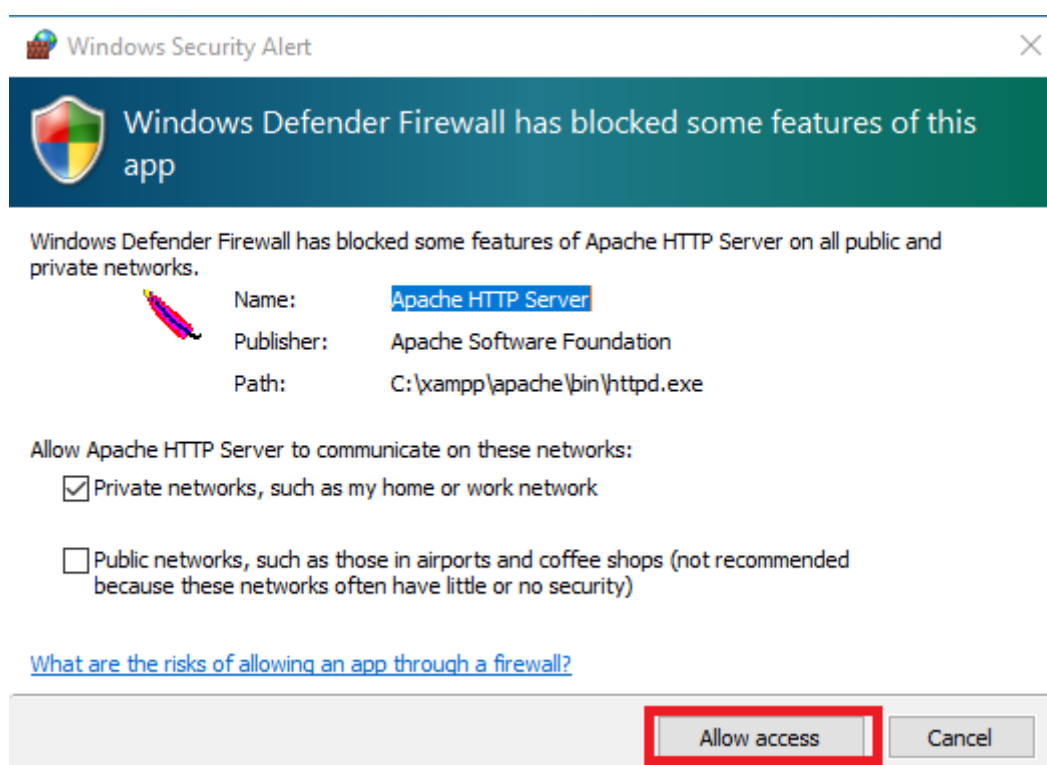
7 יש ללחוץ על **Finish** כפי שמוצג למטה.



8 יש להפעיל את Apache בפי שמוצג למטה.



9 חלון התראת האבטחה של Windows יופיע במהלך ההתקנה. יש ללחוץ על **Allow access**.



10 עכשיו Apache עובד.

XAMPP Control Panel v3.2.4 [Compiled: Jun 5th 2019]

XAMPP Control Panel v3.2.4

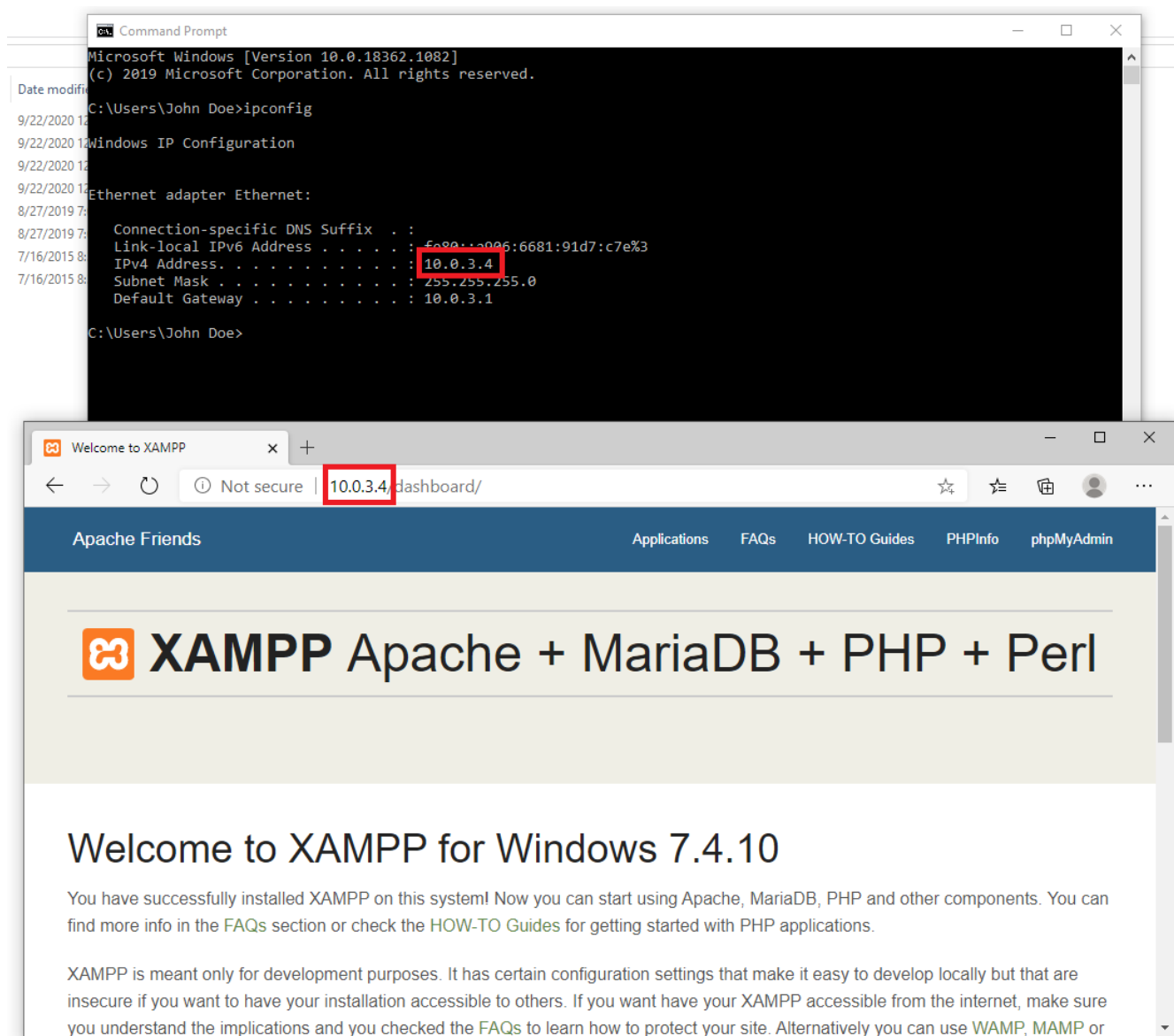
Service	Module	PID(s)	Port(s)	Actions
☒	Apache	5416 1816	80, 443	Stop Admin Config Logs
☐	MySQL			Start Admin Config Logs
☐	FileZilla			Start Admin Config Logs
☐	Mercury			Start Admin Config Logs
☐	Tomcat			Start Admin Config Logs

12:22:01 PM [main] Control Panel Ready
 12:24:02 PM [Apache] Attempting to start Apache app...
 12:24:02 PM [Apache] Status change detected: running
 12:24:11 PM [Apache] Attempting to stop Apache (PID: 2096)
 12:24:11 PM [Apache] Attempting to stop Apache (PID: 2080)
 12:24:11 PM [Apache] Status change detected: stopped
 12:24:44 PM [Apache] Attempting to start Apache app...
 12:24:44 PM [Apache] Status change detected: running

ביצוע מתקפת Dos על האתר

עכשיו נתקוף את שרת ה-Apache שהקמנו במשימה הקודמת.

- יש לפתוח את דפדפן הרשת, לפתוח את שורת הפקודה ולכתוב את כתובת ה-IP של המערכת. יש להזין את כתובת ה-IP אל דפדפן הרשת. דף האינטרנט אמור להופיע בפי שמוצג למטה.



2

כעת יש ליזום את ההתקפה על ידי הזנת הפקודה הבאה מחלון המסוף במכונה של Kali Linux:

`sudo hping3 -S 10.0.3.4 -p 80 --flood`

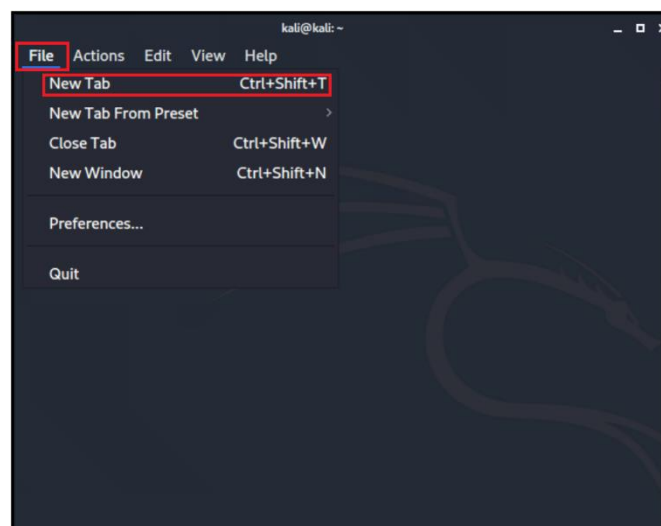
ניתן להריץ מספר פקודות hping3 להאטה נוספת של מכונת Windows 10 וזאת כדי לחקות מערכת של Botnets שתוקפים את מכונת Windows 10.

```

toor@kali: ~
File Actions Edit View Help
toor@kali:~$ sudo hping3 -S 10.0.3.4 -p 80 --flood
HPING 10.0.3.4 (eth0 10.0.3.4): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
  
```

3

כדי להריץ עוד פקודות Hping3 במסוף, יש להקליד מחדש את הפקודה בלשונית אחרת על ידי לחיצה על **File** ואז על **New Tab** או על **Ctrl+Shift+T**.



בדיקת השירות של Apache

1

כעת יש לחזור אל המכונה הווירטואלית של Windows ולנסות לרענן את חלון הדפדפן. לאחר הרענון, ניתן יהיה להבחין בסמל המסתובב ויופיע מסך ריק. התקפת ה-Dos של הצליחה!

הערה: בסופו של דבר, האתר אכן עולה, אבל לאט מאוד. הסיבה לכך היא שהמתקפה שלנו צורכת משאבי מערכת, ולמעשה מונעת שירות עבור משתמשים אמיתיים של האתר. בעולם האמיתי נשתמש במערכות רבות (בוטים) כדי למנוע מאתר Apache להעלות דפי אינטרנט בשביל המשתמשים (DDoS).

