שאלת התאוריה -

1. הסבר כיצד עובדת רשת TOR וכיצד ניתן לשמור על אנונימיות באמצעות הרשת.

TOR מסווה את כתובת ה-IP של המשתמש באמצעות שיטת שלוש הקליפות. כל בקשה לרשת האינטרנט עוברת דרך שלוש נקודות: נקודת הכניסה, נקודת מעבר ונקודת היציאה. הבקשות נעטפות כך שכל נקודה יודעת מי מאחוריה ומי לפניה, אבל לא יכולה לדעת מה תוכן הבקשה.
ניתן כך לשמור על אנונימיות מכיוון שאם נרצה לדעת מידע על כתובת ה-IP של המשתמש, נקבל גישה רק לכתובת ה-IP של נקודת היציאה. אפילו אם נצא מנקודת הנחה שנקודת היציאה שומרת את ה-IP, כל מה שהיא תוכל לתת זה את ה-IP של נקודת האמצע. נקודת האמצע תוכל לתת רק את ה-IP של נקודת הכניסה. כיוון שהנקודות פזורות על פני הגלובוס ועל פני שתיים או שלוש מדינות ורובן לא שומרות את הלוגים של ה-IP, זה הופך את מלאכת השגת הנתונים לקשה עד בלתי אפשרית.

2. הסבר כיצד עובד מנגנון הכתובות ברשת וכיצד בעצם ניגשים לאתר כלשהו.

TOR משתמש בכתובות IP המפוזרות ברחבי העולם, כך שהמקורות של שלושת כתובות ה-IP שהוא מספק יכולות להיות מפוזרות במספר מדינות וכך תורם לאנונימיות.
כלומר, ברגע שהמשתמש שולח בקשה לרשת ה-TOR היא נשלחת לנקודת כניסה, נקודת הכניסה משגרת אותה לנקודת מעבר, נקודת המעבר משגרת אותה לנקודת היציאה ונקודת היציאה משגרת אותה אל השרת. השרת מחזיר את התשובה אל נקודת היציאה, נקודת היציאה מחזירה אותה אל נקודת המעבר ונקודת המעבר מחזירה אותה אל נקודת הכניסה ורק בסוף נקודת הכניסה מחזירה את הבקשה אל המשתמש.
כתובת של אתר המשתמש בשירות הבצל מורכבת ממחרוזת של 56 אותיות ומספרים ובעלת הסיומת "onion.". **ניתן לדעת שאנו נמצאים באתר כזה בעזרת דפדפן Tor** שיראה בסרגל הכתובת צלמית של בצל המוצגת במצב הקשר כלומר, מאובטח ומשתמש בשרות בצל.

3. בהנחה וגוף מסוים בעל שליטה בשלושה צמתים של הרשת, ואדם מסוים משתמש בכל השלושה במסלולו אל היעד:
   1. האם, ואם כן כיצד ניתן לדעת שמשתמש עובר דך כל שלושת הצמתים?
   2. האם ניתן לקבל את תוכן התעבורה שלו במידה ומדובר ב-http?

1. בהנחה וגוף מסוים בעל שליטה בשלושת הצמתים **יהיה ניתן לדעת** שהמשתמש עובר דרך כל שלושת הצמתים ע"י גישה לכתובת ה-IP של היציאה אל השרת ובעזרתה מציאת כתובת ה-IP של המעבר ולבסוף לגשת לכתובת ה-IP של הכניסה ומציאת אותו אדם. אם הוא נמצא, סימון שהוא עבר דרך כל שלושת הצמתים.
2. Tor דואג להצפנת התעבורה ובנוסף גם מסתיר את התעבורה שלו ב-HTTPS רגיל כדי להקשות על איתורו. עם זאת, קיימת דרך על בסיס אלגוריתם סטטיסטי לזהות את ההתקשרויות הללו.

כתובת האתר ברשת ה-TOR:

http://vp3kzbo3ml6y7xwfosklrxdmglnbegwxh5gjlxz24r5v4nnkwx7m6qid.onion/dashboard/lhv.html

תמונה למטה -

lhv

vp3kzbo3ml6y7xwfosklrxdmglnbegwxh5gjlxz24r5v4nnkwx7m6qid.onion/dashboard/lhv.html

Hello World!

18:18
23/11/2022
ENG
חפש
18°C
מעונן רב היום