מבחן עיוני

1. ב'
2. א) השם משתמש אינו נכון.

ב) יש טעות בכתובת ה-IP.

ג) מישהו מחובר או חסם את המכונה.

3. א'

4. א) ArcSight

ב) שהוא זיהה כנראה זחלן רשת - הזחלן מתחיל את פעולתו ברשימת אתרים אותם עליו לבקר, אתרים אלו נקראים בשם "זרעים", כאשר הזחלן מבקר באתרים אלו הוא מזהה את הלינקים שיש בדף אינטרנטי מסוים ומצרף אותם לרשימת האתרים שאותם עליו לבקר. הכמות הרבה של האתרים בהם העכביש מבקר מחייבת את התוכנה לדעת לסדר את האתרים בסדר עדיפויות, אך אין אפשרות לדעת בביטחון כי האתר בו העכביש מבקר לא מבוקר בפעם הראשונה. לכן השגת מידע ראשוני בכל הפעלה של התוכנה היא דבר כמעט בלתי אפשרי. התנהגותו של הזחלן היא תוצאה של צירוף מספר קווי מדיניות:

* מדיניות של בחירה אשר מגדירה איזה עמוד להוריד.
* מדיניות של ביקור חוזר אשר מגדירה מתי לבדוק שינויים בדפים.
* מדיניות נימוס אשר מגדירה איך להימנע מעומס יתר של אתרים ולגרום להפלה של השרת.
* מדיניות של הקבלה אשר מגדירה איך לתאם בין הזחלנים השונים.

ג) כתובת המקור – במקרה זה רואים שהכתובת אינה שייכת לארגון מה שאומר שהיא כתובת שבאה מבחוץ (כנראה התוקף)

כתובת ההתקן – זה מראה את הכתובת של ההתקן המתריע (ברוב המקרים זאת תהיה הכתובת של ה- ArcSight)