

The logo features the letters 'CEH' in a large, bold, white sans-serif font. A vertical white line separates the 'C' from the 'EH'. To the right of the 'EH' is a small 'TM' trademark symbol. Behind the text is a stylized globe composed of glowing blue lines and dots, representing a network or digital sphere. Below the 'CEH' text, the words 'CERTIFIED ETHICAL HACKER' are written in a smaller, white, all-caps sans-serif font. The entire logo is set against a dark blue background with subtle circular light patterns.

[illegible][illegible]

<https://www.isc2.org/ethics/default.aspx>

1. **Цель и задачи исследования.** Целью исследования является изучение влияния различных факторов на эффективность работы системы управления качеством (СУК) в организации. Задачами исследования являются:

[illegible]

Electronic Communication Privacy Act

Computer Fraud and Abuse Act of 1984

The Cyber Security Enhancement Act of 2002

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001

The Federal Information Security Management Act

Federal Sentencing Guidelines of 1991

Economic Espionage Act of 1996

.0000 0000 00 0000 00000000 0000 000000 000000 000000 00 000000 000000 000000 000000 000000 000000 000000

□ □ □ □ □ □ □ □ □ □ □ □ □ □

[illegible][illegible][illegible]

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □

[illegible]

אנו יודעים כי ישנם סכנים רבים הקשורים בשימוש בשרתים. לדוגמה, סכנת התקפות ממוקדות, סכנת גנבת נתונים, סכנת הפרת פרטיות וכו'. לכן, חשוב מאוד להבטיח את אבטחת השרתים. אחת הדרכים להבטיח את אבטחת השרתים היא באמצעות שימוש ב-IDS (Intrusion Detection System). IDS הוא מערכת המיועדת לזיהוי התקפות ופגיעות בשרתים. היא עובדת על ידי מעקב אחר התנועה הרשתית וזיהוי פעילות חשודה. לדוגמה, אם ישנה התקפה ממוקדת על שרת, IDS יזהה זאת ויודיע למנהל השרת. בנוסף, ישנן דרכים אחרות להבטיח את אבטחת השרתים, כגון: שימוש באמצעי אבטחה נוספים, מעדכן תוכנות, וכו'. חשוב מאוד להבטיח את אבטחת השרתים, מכיוון ששרתים מכילים נתונים חשובים ויכולים לגרום נזק רב אם ייחשפו. לכן, יש להקדיש תשומת לב מיוחדת לאבטחת השרתים. <http://www.exploit-db.com> הוא אתר המספק מידע על פגיעות ודרכי התקפות. אתר זה יכול להיות שימושי מאוד למנהלי שרתים.

ישנן דרכים רבות להבטיח את אבטחת השרתים. אחת הדרכים היא באמצעות שימוש ב-(deny) ספיגת גישה. דרך זו עובדת על ידי ספיגת גישה לשרתים מכתובות IP חשודות. לדוגמה, אם ישנה התקפה ממוקדת על שרת, ניתן לספק את כתובת ה-IP של התוקף לרשימת הספיגה. דרך זו יכולה להיות שימושית מאוד.

ישנן דרכים רבות להבטיח את אבטחת השרתים. אחת הדרכים היא באמצעות שימוש ב-OpenVAS. OpenVAS הוא מערכת המיועדת לזיהוי פגיעות בשרתים. היא עובדת על ידי מעקב אחר התנועה הרשתית וזיהוי פעילות חשודה. לדוגמה, אם ישנה פגיעה בשרת, OpenVAS יזהה זאת ויודיע למנהל השרת. בנוסף, ישנן דרכים אחרות להבטיח את אבטחת השרתים, כגון: שימוש באמצעי אבטחה נוספים, מעדכן תוכנות, וכו'. חשוב מאוד להבטיח את אבטחת השרתים, מכיוון ששרתים מכילים נתונים חשובים ויכולים לגרום נזק רב אם ייחשפו. לכן, יש להקדיש תשומת לב מיוחדת לאבטחת השרתים.

(Gaining Access) **השגת גישה** / **השגת זכויות**

השגת גישה לשרת היא אחד מהשלבים החשובים ביותר בתהליך ההתקפה. ישנן דרכים רבות להשיג גישה לשרת, כגון: שימוש באמצעי אבטחה, שימוש ב-SSH, שימוש ב-FTP, וכו'. אחת הדרכים להשיג גישה לשרת היא באמצעות שימוש באמצעי אבטחה. לדוגמה, אם ישנה פגיעה בשרת, ניתן להשתמש באמצעי אבטחה כדי להשיג גישה לשרת. דרך זו יכולה להיות שימושית מאוד. בנוסף, ישנן דרכים אחרות להשיג גישה לשרת, כגון: שימוש ב-SSH, שימוש ב-FTP, וכו'. חשוב מאוד להבטיח את אבטחת השרתים, מכיוון ששרתים מכילים נתונים חשובים ויכולים לגרום נזק רב אם ייחשפו. לכן, יש להקדיש תשומת לב מיוחדת לאבטחת השרתים.

השגת גישה לשרת היא אחד מהשלבים החשובים ביותר בתהליך ההתקפה. ישנן דרכים רבות להשיג גישה לשרת, כגון: שימוש באמצעי אבטחה, שימוש ב-SSH, שימוש ב-FTP, וכו'. אחת הדרכים להשיג גישה לשרת היא באמצעות שימוש באמצעי אבטחה. לדוגמה, אם ישנה פגיעה בשרת, ניתן להשתמש באמצעי אבטחה כדי להשיג גישה לשרת. דרך זו יכולה להיות שימושית מאוד. בנוסף, ישנן דרכים אחרות להשיג גישה לשרת, כגון: שימוש ב-SSH, שימוש ב-FTP, וכו'. חשוב מאוד להבטיח את אבטחת השרתים, מכיוון ששרתים מכילים נתונים חשובים ויכולים לגרום נזק רב אם ייחשפו. לכן, יש להקדיש תשומת לב מיוחדת לאבטחת השרתים.

(Privilege escalation) **השגת זכויות**

השגת זכויות לשרת היא אחד מהשלבים החשובים ביותר בתהליך ההתקפה. ישנן דרכים רבות להשיג זכויות לשרת, כגון: שימוש באמצעי אבטחה, שימוש ב-SSH, שימוש ב-FTP, וכו'. אחת הדרכים להשיג זכויות לשרת היא באמצעות שימוש באמצעי אבטחה. לדוגמה, אם ישנה פגיעה בשרת, ניתן להשתמש באמצעי אבטחה כדי להשיג זכויות לשרת. דרך זו יכולה להיות שימושית מאוד. בנוסף, ישנן דרכים אחרות להשיג זכויות לשרת, כגון: שימוש ב-SSH, שימוש ב-FTP, וכו'. חשוב מאוד להבטיח את אבטחת השרתים, מכיוון ששרתים מכילים נתונים חשובים ויכולים לגרום נזק רב אם ייחשפו. לכן, יש להקדיש תשומת לב מיוחדת לאבטחת השרתים.

[illegible]