| הפרק המופיע בתוכנית הלימודים | פירוט תכנים והבהרות בפרק |
|---|---|
| **פרק 1 יסודות האבטחה ברשת תקשורת**<br>מטרת הפרק<br>להכיר להסביר ולתאר את האיומים ברשתות תקשורת.<br>פירוט התכנים<br>•התלמיד יתאר ויסביר את עקרונות היסוד באבטחת רשת.<br>•התלמיד יתאר ויסביר את ההבדלים בין וירוס, תולעת, וסוס טרויאני.<br>•התלמיד יתאר מתודולוגיות תקיפה.<br>Reconnaissance, Access, Denial of Service, and DDoS<br>•התלמיד יתאר את מסגרות ההגנה הבסיסיות הכוללות בקרה וניהול של העברת נתונים | **<u>מטרת הפרק</u>**<br>להכיר להסביר ולתאר את האיומים ברשתות תקשורת.<br>**<u>פירוט התכנים</u>**<br>*התלמיד יתאר ויסביר את עקרונות היסוד באבטחת רשת. –<br>.Confidentiality, Integrity, and Availability<br>*התלמיד יתאר ויסביר את המושגים הבאים:<br>Asset, Vulnerability, Thret, Risk and Countermeasure.<br>התלמיד ידע לתאר ולהסביר מי הם הגורמים שיכולים לתקוף את הרשת: טרוריסטים, פושעים, סוכנויות ממשלתיות, מדינות, פצחנים, עובדים ממורמרים, מתחרים וכל אחד עם גישה למחשב.<br>התלמיד יתאר ויסביר את ההבדלים בין וירוס, תולעת, וסוס טרויאני.<br>התלמיד יתאר שיטות תקיפה ( בכללי , אין צורך לדעת לתקוף רק לתאר מה היא ההתקפה): Reconnaissance, Social Engineering, Privilege escalation, Back doors, Code execution, Covert Channel, Trust exploitation, Brute-force, Botnet, DoS, DDoS<br>התלמיד יתאר ויסביר מהי מפת האיומים הכללית מבחינת אבטחת מידע: Financial, Disruption, Geopolitical |

| הפרק המופיע בתוכנית הלימודים | פירוט תכנים והבהרות בפרק |
|---|---|
| | התלמיד יתאר ויסביר מהי התקפת DDoS על סוגיה : Direct, Reflected, Amplification.<br>התלמיד יסביר מהם התקפות של הנדסה חברתית כמו Phishing, Malversating, Phone scam.<br>התלמיד ידע באיזה שיטות להתמודד עם הנדסה חברתית : Password Management, Two-factor authentication, Antivirus, Antiphishing, Information classification, Document handling.<br>התלמיד יתאר ויסביר (בכללי לא לעומק) מהם השיטות לזהות נוזקות : Packet captures, Snort, NetFlow, IPS |
| **פרק 2 יסודות אבטחה של רכיבי תקשורת**<br>מטרת הפרק<br><br>להכיר ולממש אבטחה של רכיבי תקשורת.<br>פירוט התכנים<br>תלמיד יסביר ויגדיר אבטחה בסיסית לגישה, ישירה ומרחוק, אל רכיבי תקשורת.<br>התלמיד יגדיר חוקיות הרשאות ניהול.<br>התלמיד יוכיח יכולות ניטור וניהול רכיבים על ידי מימוש אבטחת וניהול מעקב.<br>התלמיד יוכיח יכול להשתמש באמצעים אוטומטיים של רכיבי התקשורת לניטור מידע. | **<u>מטרת הפרק</u>**<br>להכיר שיקולי אבטחה ברשת המקומית.<br>להכיר אפשרויות הטמעה של אבטחה ברכיבי קצה ברשת מקומית.<br>להכיר אפשרויות אבטחה בשכבה 2.<br>**<u>פירוט התכנים</u>**<br>**יסודות : VLAN and Trunking**<br>התלמיד יתאר ויסביר מהו VLAN.<br>התלמיד ידע להגדיר VLAN על גבי מתגים. |

| הפרק המופיע בתוכנית הלימודים | פירוט תכנים והבהרות בפרק |
|---|---|
| | התלמיד יתאר ויסביר מהו Trunk ומהו פרוטוקול 802.1Q<br>התלמיד יתאר ויסביר מהו ה-Native VLAN.<br>התלמיד יתאר ויסביר מה זה Inter-VLAN Routing.<br>התלמיד יתאר ויסביר מהו תת ממשק וירטואלי Virtual SUB interface.<br>**יסודות STP.**<br>התלמיד יתאר ויסביר מהו פרוטוקול STP ומה התפקיד שלו.<br>התלמיד יתאר ויסביר מהן לולאות מיתוג ומה רע בהן.<br>התלמיד יתאר ויסביר מה הפתרון ללולאות מיתוג : STP או 802.1D.<br>התלמיד יתאר ויסביר את המושגים Root Port, Designated ו-Nondesignated .<br>התלמיד יתאר ויסביר מה השימוש ומתי נעשה שימוש ב-portfast.<br>התלמיד יתאר ויסביר מה השימוש ומתי נעשה שימוש ב-Rapid Spanning Tree.<br>התלמיד יכיר את ההמלצות (Best Practices) הקשורות לשכבה 2.<br>התלמיד יכיר יתאר וידע להגדיר את כלי האבטחה של שכבה 2 :<br>Port security<br>BPDU Guard<br>Root Guard<br>Dynamic ARP inspection |

| הפרק המופיע בתוכנית הלימודים | פירוט תכנים והבהרות בפרק |
|---|---|
| | IP Source Guard<br>Storm control<br>Access control lists<br>התלמיד יתאר יסביר וידע לאבטח את הפרוטוקולים CDP ו-LLDP.<br>התלמיד יכיר יתאר וידע להגדיר DHCP Snooping. |
| **פרק 3 – AAA Authentication, Authorization, and Accounting**<br>מטרת הפרק<br>.<br>להכיר ולממש ניהול גישה לרכיבי רשת באמצעות מתודתAAA<br>פירוט התכנים<br>• תלמיד יסביר את הנחיצות של פרוטוקולים למימוש AAA .<br>• התלמיד יממש AAA על נתב, באמצעות שימוש בבסיס נתונים של הנתב.<br>• התלמיד יממש שרת מבוסס AAA.<br>• התלמיד יממש שרת אימות מבוסס AAA , באמצעות פרוטוקולים. TACACS+ , RADIUS<br>• התלמיד יממש שרת מבוסס AAA , לניהול הרשאות וניהול חשבונות משתמשים. | **מטרת הפרק**<br>להכיר ולממש ניהול גישה לרכיבי רשת באמצעות מתודתAAA<br>**פירוט התכנים**<br>• התלמיד יסביר מהם הפרוטוקולים המשמשים ליישום מתודת AAA.<br>TACACS+, RADIUS.<br>• התלמיד יסביר את ההבדל בין הפרוטוקולים למימוש AAA. TACACS+ אל מול RADIUS.<br>• התלמיד יממש AAA על נתב, באמצעות שימוש בבסיס הנתונים של הנתב.<br>• התלמיד יממש שרת אימות מבוסס AAA , באמצעות פרוטוקולים , TACACS+<br>RADIUS . |

| הפרק המופיע בתוכנית הלימודים | פירוט תכנים והבהרות בפרק |
|---|---|
| | • התלמיד יממש שרת מבוסס AAA לניהול הרשאות וניהול חשבונות משתמשים – נושא זה הוא לא חובה. לשיקול המורה והוא איננו כלול בנושאי הבחינה<br>• התלמיד יפעיל שיטות להתמודדות עם תקלות: בדיקת תקשורת מול שרת על ידי פינג, הפקודה test aaa (לא נתמך על ידי PT) , debug, show users.<br>• פקודות למימוש:<br>o aaa new-model<br>o aaa authentication login AUTHEN_via_TACACS group tacacs+ local<br>o aaa authorization exec Author-Exec_via_TACACS group tacacs+ local<br>o username admin privilege 15 secret cisco<br>o tacacs-server host 192.168.1.252 key cisco123<br>o R1(config-line)# login authentication AUTHEN_via_TACACS<br>o R1# debug aaa authentication<br>o test aaa group tacacs+ admin cisco123 legacy |

| הפרק המופיע בתוכנית הלימודים | פירוט תכנים והבהרות בפרק |
|---|---|
| **פרק 4 מימוש חומת אש**<br>מטרת הפרק<br>.<br>להכיר טכנולוגיות של חומת אש, להגנה על הכניסות לרשת.<br>פירוט התכנים<br>. ACL •התלמיד יכיר ויסביר את הסוגים השונים של רשימות גישה .<br>–<br>•התלמיד יסביר כיצד רשימת גישה מאפשרת למנוע חדירות.<br>•התלמיד יגדיר ויממש חומת אש, למנוע חדירות והתקפות.<br>•התלמיד יגדיר מדיניות חומת אש מבוססת אזור מוגדר ברשת. | • התלמיד יכיר ויסביר את השיטות השונות להפעלת חומת אש( firewall methodologies) . **על התלמיד להבין את ההבדלים ואת היתרונות והחסרונות בין היכולות של כל סוג של חומת אש.**<br>○ Simple packet-filtering techniques<br>○ Proxy servers (also known as *application layer gateway [ALG]*)<br>○ Stateful inspection firewalls<br>○ Transparent firewalls<br>○ Next-generation context and application-aware firewalls<br>• התלמיד ידע להסביר ולהגדיר רשימות גישה סטנדרטיות של IPv4.<br>• התלמיד ידע להגדיר גישה מאובטחת לפורטים של VTY על ידי רשימות גישה סטנדרטיות של IPv4.<br>• התלמיד ידע להסביר ולהגדיר רשימות גישה מורחבות של IPv4<br>• התלמיד ידע להסביר ולהגדיר רשימות גישה ממוספרות (Numbered ACL)<br>• התלמיד ידע להסביר ולהגדיר רשימות גישה שמיות (Named ACL)<br>• התלמיד ידע להסביר ולהגדיר רשימות גישה מורחבות מהסוגים הבאים:<br>○ Numbered<br>○ Established<br>○ מבוססות פורטים ופרוטוקולים |
| **פרק 5 מימוש הגנה מפני חדירות לרשת–**<br>מטרת הפרק<br>.<br>להכיר שיטות להגדרת IPS כדי להפחית חדירות והתקפות על הרשת.<br>פירוט התכנים<br>. •התלמיד יכיר ויסביר טכנולוגיות IPS.<br>•התלמיד יסביר שיטות להבחין בחדירות לרשת.<br>•התלמיד יסביר שיטות למניעת חדירות לרשת.<br>•התלמיד יכיר יתאר ויסביר נחיצות של חתימות דיגיטליות, כדי לזהות תעבורה זדונית.<br>•התלמיד יממש התקנה והגדרה של , IPS תוך שימוש ב , CLI - ו - CCP | • התלמיד ידע להסביר מה ההבדל בין IPS ל-IDS מהבחינות הבאות:<br>○ המיקום ב"זרימה" של הרשת<br>○ תצורה (Promiscuous או inline)<br>○ Latency or Delay<br>○ התלמיד ידע להסביר מהו Sensor<br>○ מה ההשפעה כאשר הסנסור לא מצליח להעביר חבילות מידע<br>○ מניעת כניסה של תעבורה זדונית<br>• סוגי הסנסורים הקיימים<br>• התלמיד ידע להסביר כיצד מזהים תעבודה זדונית ברשת<br>○ Signature-based IPS/IDS<br>○ Policy-based IPS/IDS<br>○ Anomaly-based IPS/IDS<br>○ Reputation-based IPS/IDS |

| הפרק המופיע בתוכנית הלימודים | פירוט תכנים והבהרות בפרק |
|---|---|
| •התלמיד יוכיח יכולת אימות וניטור IPS על ידי שימוש ב. CLI - | |
| **פרק 6 אבטחת הרשת המקומית**<br><br>מטרת הפרק<br>.<br>להכיר שיקולי אבטחה ברשת המקומית.<br>להכיר אפשרויות הטמעה של אבטחה ברכיבי קצה ברשת מקומית.<br>להכיר אפשרויות אבטחה בשכבה 2.<br>פירוט התכנים<br>•התלמיד יתאר ויסביר את נקודות התורפה של רכיבי קצה.<br>•התלמיד יתאר את אמצעי ההגנה האפשריים על רכיבי קצה<br>•התלמיד יתאר ויסביר נקודות תורפה של שכבה 2.<br>•התלמיד יתאר ויסביר אפשרויות הגנה על שכבה 2.<br>•התלמיד יגדיר הגנה על מתג כולל הגנת פורטים.<br>•התלמיד יתאר ויסביר שיקולי אבטחה ברשת , VOIP , WIFI<br>SAN . | מטרת הפרק<br>• התלמיד יתאר ויסביר את שלושת המושגים הבאים : Management plane, Control plane ו-Data plane.<br>• התלמיד יתאר יסביר וידע ליישם אבטחה בכל אחד מהמישורים :<br>○ מישור הניהול : AAA, NTP, SSH,SNMPv3<br>○ מישור הבקרה : אימות בזמן שימוש בפרוטוקולי ניתוב.<br>○ מישור המידע : ACL, Privet VLAN, STP Guards, IOS IPS, ZBF.<br>• התלמיד יתאר ויסביר את ה-Best Practices עבור ההגנה של כל אחד מהמישורים.<br>• התלמיד יתאר ויסביר את נקודות התורפה של רכיבי קצה.<br>• התלמיד יתאר את אמצעי ההגנה האפשריים על רכיבי קצה<br>• התלמיד יתאר ויסביר נקודות תורפה של שכבה 2.<br>• התלמיד יתאר ויסביר אפשרויות הגנה על שכבה 2.<br>• התלמיד יגדיר הגנה על מתג כולל הגנת פורטים. |

| הפרק המופיע בתוכנית הלימודים | פירוט תכנים והבהרות בפרק |
|---|---|
| | • התלמיד יתאר ויסביר שיקולי אבטחה ברשת. WIFI , VOIP , SAN |
| **פרק 7 מערכות הצפנה**<br><br>מטרת הפרק<br>• להכיר שיטות הגנה על מידע.<br>• להכיר שיטות אימות מקור של מידע.<br>פירוט התכנים<br>• התלמיד יכיר ויתאר, שירותים ושיטות להצפנת מידע.<br>• התלמיד יתאר ויסביר ערבול מידע. hashing ,<br>• התלמיד יסביר מהי ומה תפקידה של חתימה דיגיטלית.<br>• התלמיד יסביר כיצד הצפנה, ערבול, וחתימה דיגיטלית מאפשרות אימות סודיות ויושרה.<br>• התלמיד יתאר ויסביר את המנגנונים המשמשים להבטיח שלמות נתונים ואימות<br>• התלמיד יתאר את המנגנונים המשמשים להבטיח סודיות נתונים.<br>• התלמיד יתאר וידגים, את המנגנונים המשמשים בקריפטוגרפיה של זוג מפתחות ציבורי ופרטי. | **<u>מטרת הפרק</u>**<br>**להכיר את טכנולוגיות ההצפנה**. (Fundamentals of VPN Technology and Cryptography)<br>**<u>פירוט התכנים</u>**<br>• התלמיד יתאר ויסביר מהו צופן<br>• התלמיד יתאר ויסביר מהם הצפנים מהסוגים הבאים: Substitution, Polyalphabetic, Transposition.<br>• התלמיד יסביר מה ההבדל בין Block Ciphers ו-Stream Ciphers<br>• התלמיד יתאר ויסביר מהן אלגוריתם סימטרי מול אסימטרי.<br>• התלמיד יכיר את האלגוריתמים הסימטריים: DES, 3DES, AES, IDEA, RC2, RC4, RC5, RC6, Blowfish.<br>• התלמיד יכיר את האלגוריתמים האסימטריים: RSA, DH, ElGamal.<br>• התלמיד יסביר ויתאר מהו גיבוב ולשם מה הוא משמש. |

| הפרק המופיע בתוכנית הלימודים | פירוט תכנים והבהרות בפרק |
|---|---|
| | • התלמיד יכיר וידע מה ההבדלים בין שיטות הגיבוב הבאות : MD5, SHA-1, SHA2.<br>• התלמיד יסביר ויתאר מהי חתימה דיגיטאלית וכיצד היא עובדת.<br>• התלמיד יתאר ויסביר מהי חבילת הפרוטוקולים והאלגוריתמים של IPsec.<br>• התלמיד יתאר ויסביר מהם שתי השיטות המרכזיות למימוש IPsec : ESP ו-AH.<br>• התלמיד יתאר ויסביר מהם שיטות ההצפנה המשמשות IPsec : DES, 3DES ו-AES.<br>• התלמיד יתאר ויסביר מהם שיטות הגיבוב המשמשות IPsec : MD5 ו- SHA.<br>• התלמיד יתאר ויסביר מהם האלגוריתמים המשמשים לאימות ב-IPsec : PSK ו-RSA.<br>• התלמיד יתאר ויסביר מהן השיטות לניהול מפתחות : DH, PKI ו-IKE.<br>• התלמיד יתאר ויסביר מה זה SSL ולאיזה מטרות משמש.<br>• התלמיד יתאר ויסביר את מהי חתימה דיגיטלית ולאיזו מטרה היא משמשת. |
| **פרק 8 מימוש VPN**<br>מטרת הפרק<br>• להכיר את היתרונות של רשת פרטית וירטואלית. VPN<br>• להכיר שיטות הגדרה של. VPN | **מטרת הפרק** |

| הפרק המופיע בתוכנית הלימודים | פירוט תכנים והבהרות בפרק |
|---|---|
| פירוט התכנים<br>• התלמיד יתאר מהי רשת וירטואלית פרטית.<br>• התלמיד יסביר את הנחיצות של. VPN<br>• התלמיד יגדיר ויממש VPN GRE אתר לאתר site to ( . site .)<br>• התלמיד יתאר את רכיבי IPSec שך , VPN ויסביר את פעולתם.<br>• התלמיד יגדיר ויאמת site-to-site IPSec VPN עם שיתוף מפתח אימות, על ידי. CLI<br>• התלמיד יממש ויאמת site-to-site IPSec VPN תוך שימוש ב. CCP -<br>• התלמיד יממש ויאמת גישה מרחוק ל. VPN - | • להכיר את היסודות של רשתות VPN ושל טכנולוגיות הצפנה<br>• להכיר דרכי הגדרה של VPN .<br>• הקמת Site-To-Site VPN על גבי נתבים.<br>• הכרות והבנת IPsec<br>**<u>פירוט התכנים</u>**<br>• התלמיד יתאר מהי רשת וירטואלית פרטית.<br>• התלמיד יתאר ויסביר את היתרונות של רשתות VPN : Confidentiality, Data integrity, Authentication, Antireplay protection.<br>• התלמיד יתאר את סוגי ה- VPN הבאים : IPsec, SSL, MPLS<br>• התלמיד יתאר את מהם ומה ההבדלים בין Remote-access VPN ל- Site-to-Site VPN.<br>• התלמיד יסביר את הנחיצות של. VPN<br>• התלמיד יתאר ויסביר מה השימוש ומה ההבדל בין Site-To-Site VPN ל--Remote Access VPN. |

| הפרק המופיע בתוכנית הלימודים | פירוט תכנים והבהרות בפרק |
|---|---|
| | • התלמיד יסביר מה המטרות של IPsec ובאיזה שיטה מטרות אלו ממומשות: סודיות על ידי הצפנה, אמינות על ידי גיבוב, אימות עמיתים על ידי PSK ועל ידי חתימות דיגיטליות RSA ומניעת חזרות (מוטמע בתוך IPsec).<br>• התלמיד יתאר ויסביר מהו פרוטוקול IKE<br>• התלמיד יתאר ויסביר מה קורה בשלבים של IKE Phase 1 ו-IKE Phase 2.<br>• התלמיד יממש יגדיר ויבדוק תקינות של Site-to-Site , IPsec VPN בין 2 נתבים על ידי ה-CLI.<br>• התלמיד יתאר ויסביר מה המהות והצורך של פרוטוקול GRE ומה השימוש ב-GRE over IPsec.<br>• התלמיד יתאר ויסביר מהו Tunnel Interface (מסוג GRE).<br>• התלמיד יגדיר ויממש VPN המממש GRE over IPsec.<br>• התלמיד ידע להסביר ולהשתמש בפקודות SHOW רלוונטיות לאיתור תקלות בתעלות IPsec ( show crypto isakmp sa, show crypto ikev2 sa, show crypto ikev2 sa detailed, show crypto ikev2 session)<br>• |
| **פרק 9 מימוש ASA** | |

הפרק המופיע בתוכנית הלימודים

| מטרת הפרק |
| --- |
| התלמיד יכיר שיטות תיעוד של מטרות האבטחה בארגון.<br>התלמיד יכיר דרכים לממש אבטחה בהינתן מטרות.<br>התלמיד יכיר שיטות לממש מדיניות אבטחה מותאמות לארגון.<br>פירוט התכנים<br>•התלמיד יתאר שיטות להקמת חומת אש מתקדמת.<br>•התלמיד יסביר כיצד טכנולוגית , ASA מממשת חומת אש יעילה.<br>•התלמיד יגדיר ויממש חומת אש מטיפוס. ASA<br>•התלמיד יגדיר ויממש גישה מרחוק ל VPN - על. ASA |

פירוט תכנים והבהרות בפרק

| מטרת הפרק |
| --- |
| • הקמת Site-To-Site VPN על גבי ASA.<br>• הקמת Remote-Access VPNs על גבי ASA |