איתי חורי

itay@huri.biz

נסיון מקצועי

CLOUDINFECT/SNDBOX – 2017-PRESENT

סטארטאפ בתחום הסייבר, פלטפורמת מחקר מעמיק של קבצים הממונעת AI.
Full-stack developer, אחראי על מגוון תחומים החל מהמחקר והתכנון, לפיתוח של האפליקציה ועד ל-deployment.

- אפיון, תכנון ופתרון בעיות מורכבות ב-scale
- פיתוח Back end עם Node.js ,Python, ES7, Babel, ESlint, Webpack
- עבודה עם Docker וה-Stack ב-AWS: ElasticBeanstalk, S3, ELB, ECS, Cloudfront, SQS, SNS ו-Lambda
- פיתוח Front end עם Vue.js, SASS ו-אינטגרציה עם UI/UX
- אדמיניסטרציית שרתי החברה, עבודה עם Ansible
- ארכיטקטורת Cloud
- זיהוי תפוסי התהגות חשודים במערכת מנוטרת, עבודה עם network dumps, IDS

VDOS STRESS TESTING SOLUTIONS – 2014-2016

עצמאי. סימולצית התקפות סייבר בזמן אמת, נועד לבחון את אבטחת הרשת בפני איומי התקפות DDoS שונות.

- ניהול ישיר של צוות מתכנתים וחברי תמיכה טכנית.
- עבודה בסביבת Windows, Linux(CentOS, Ubuntu) ו- MacOS.
- פיתוח Front end עם Javascript, CSS3, Vue.js, jQuery, SASS, Bootstrap ומתולוגיית BEM.
- פיתוח Back end עם Node.js, PHP ונסיון עם Express.js, Laravel וארכיטקטורת MVC.
- נסיון עם פיתוח Test-driven.
- כתיבת סקריפטים ב-bash ו-Python.
- Version control עם git ועבודה עם GitHub ו-GitLab.
- נסיון עם פלטפורמות ותשתיות ענן Digitalocean, AWS ו-Heroku.
- נסיון עם DNS management ו-WAF.
- עיסוק עם פרוטוקולי TCP/IP.
- קינפוג ועבודה מול מסדי נתונים מסוג MySQL ושרתי Web מסוג Nginx ו-Apache.
- עיסוק בפיתוח רב תחומי של מערכות ובניהם: מערכות מניעת הונאה בכרטיסי אשראי, מחקר חולשות ופרוטוקולי אינטרנט.
- פיתוח ושימוש ב-RESTful APIs.
- נסיון עם Stripe, Braintree ו-PayPal , והטמעה שלהן במערכות.

FREELANCER – 2013-2014

שימשתי כ-Freelancer, מפתח אתרים ב-LAMP Stack וכמאבטח אתרים כנגד פרצות שונות כדוגמת:
SQL injection, Session spoofing, Cross Site Scripting, Remote / Local file inclusion, Remote Code Execution, HTTP Response Splitting, Extension Spoofing, SQL DoS.

השכלה

2013-2016 – תיכון ע"ש מוסינזון

אוטודידקט, למדתי תחומים שונים באמצעות אתרי אינטרנט וספרים.

השכלה תיכונית, תיכון מוסינזון שבהוד השרון, מגמת אלקטרוניקה ומחשבים, ציון סופי 98, בגרות מלאה.

תוכן לקריאה שכתבתי

מתקפות מניעת שירות מוגברות - מגזין אבטחת מידע DIGITALWHISPER.CO.IL

מגמת הצמיחה ההולכת וגוברת של רשת האינטרנט משכה חברות, ארגונים גדולים וממשלות לשימוש במערכות מחשב. עם צמיחת האינטרנט, האקרים פתחו מיומניות להשבתת המערכות האלה. בהתקפת מניעת שירות (DoS / DDoS). במאמר זה אציג מתקפות מניעת שירות מוגברות - אשר מאפשרות ליזום מתקפות מניעת שירות אפקטיביות גם עם משאבים מוגבלים, ע"י ניצול פרוטוקולי UDP כגון DNS ו-NTP. במאמר מממש את סקריפט ההתקפה בשפת Python.

דוגמאות לפרוייקטים שפיתחתי

NOVA VPN

מטרת הפרוייקט היא לספק למשתמש חוויית אנונימיות מקסימלית והגנה ממתקפות ברשת לוקאלית, לדוגמא MITM. התוצאה מבוצעת ע"י הצפנת התעבורה בין המשתמש לשרת מייפה כוח, כך שהמשתמש יוכל לגלוש באינטרנט בצורה אנונימית לחלוטין. בנוסף, בתוך הרשת הוירטואלית נמצא שרת DNS שמאזין לבקשות DNS זדוניות, לדוגמא - שרתי פרסומות (לדוגמא שרתי Google Ads), שרתי Tracking (לדוגמא, Google Analyrics), ו-Malware. וחוסם אותן לחלוטין, ובנוסף מבצע Chaching לצורך האצת מהירות גלישה. השרת הממפה בין בקשות שנחסמו לבין משתמש ספיציפי, אוגר נתונים על כמות הבקשות שנחסמו לכל משתמש ושולח אותה לשרת ה-WEB. לאחר מכן כל משתמש יכול לצפות בסטטיסטיקות של כמה איומים ה-VPN חסם בדף הבית. הפרוייקט נגיש בכתובת novavpn.net.
פותח ב-Laravel PHP framework ו-Python תוך כדי אוטומטציה ל-OpenVPN.
scaleable ומאוחסן על Elastic Beanstalk של AWS.

SECRET

כלי קוד פתוח המאפשר שליחת פתקים המושמדים אוטומטית לאחר קריאתם ומוצפנים עם AES. לאחר הקלדת תוכן הפתק באתר, יווצר מפתח רנדומאלי ב-client side, ובעזרתו תוכן הפתק יוצפן וייאוחסן ללא המפתח בשרת. הלקוח מקבל לינק אותו הוא יכול להפיץ המכיל את מפתח ההצפנה כ-hash parameter אשר לא יעזוב את הדפדפן בפעולת הפענוח, אשר נעשית גם כן כולה ב-client side.
הפרוייקט נגיש בכתובת secret.huri.biz
פותח עם Vue.js, Node.js ו-MongoDB ולגמריי serverless ו-scaleable.
מאוחסן על AWS API Gateway, Lambda, S3, Cloudfront.

מטרת הפרויקט היא האזנה למסך מחשב ושליטה בו, כל 100 מילישניות נשלח פריים של המסך לשרת HTTP, השרת HTTP מקבל את הפריים, מקודד ב-base64, השרת מכניס את הפריים למסד נתונים (כך שבנוסף תהיה אופציה לצפייה בהיסטורית המסך של המשתמש) ובאתר יש אפשרות לצפייה בפריימים קודמים וצפייה במסך של המשתמש בlive. בנוסף, הקליינט מאזין לשרת HTTP ומקבל ממנו פקודות, לדוגמא, הורדה של קובץ, הפעלה, וסיפוק מידע חי על המערכת.
פותח ב-Vanilla PHP ו-Python.

שפות

עברית – כתיבה, קריאה ודיבור – שפת אם
אנגלית – כתיבה וקריאה – רמת שפת אם