שלב ג'

פיתחתם מערכת רצינית מאוד של שרת תוקף ומחשב מותקף. על מנת להעלות את הרמה ולשדרג את המערכת עוד יותר, נצלול כעת לדברים המצריכים הבנה יותר עמוקה של המערכת. אם מדובר על הנדוס לאחור או על ניתוח של חבילות (פקטות). בשלבים אלו יהיה עליכם להשלים את הידע החסר לכם באמצעות מחקר ואיך לא, ניסוי ותהייה.

תזכורת הנחיות

- אתם יכולים להשתמש באילו שפות תכנות שתרצו - מומלץ לקרוא היטב את ההנחיות ולחשוב מה תהיה שפת המימוש המתאימה ביותר.
- על הקוד שלכם להיות מתועד להפליא. תמיד תחשבו על היום שתגייסו עובד שימשיך את הפיתוח של מה שבניתם ואנו מבטיחים לכם שלא תרצו שבכל דבר שלא ברור לו או לה הם יבואו לשאול אתכם מה עשיתם - תעדו היטב את הקוד!
- העבודה בצוות צריכה לעזור לכם ולכן חשבו היטב כיצד לחלק את העבודה, הגדירו מראש שיטות עבודה, חתימות לפונקציות וכל דבר אחר שיחסוך בעיות בשלב חיבור החלקים השונים שפיתחתם.
- התחילו בקריאה והבנה של המשימות. חשבו והשתמשו באינטרנט על מנת להבין אילו שפות תכנות מכילות את הספריות המתאימות שיעזרו לכם לממש בצורה מהירה, יעילה ומיטבית את מה שאתם צריכים. לפעמים מדובר בהבדלים משמעותיים.
- כאשר השלמתם את השלב ואתם מרגישים טוב עם עבודתכם, יש להציג למדריך על מנת לעבור לשלב הבא.

תרגיל 9:

הבסיס לביצוע מתקפות ברשת הפנימית של המחשב המותקף, הוא להבין את הטופולוגיה של הרשת ולהכיר את המחשבים האחרים שמחוברים לרשת הזאת. בהרבה מצבים בהם אנחנו רוצים להגיע למחשב כלשהו בתוך ארגון, נחפש את היחידה הכי פחות מוגנת באותו ארגון ונתקין עליה את הנוזקה שבנינו. היכולת להתקדם בתוך הרשת הפנימית מפחיתה משמעותית את מנגנוני ההגנה וזה מקל עלינו. לאור זאת, בשלב זה אנחנו רוצים לקבל את מפת ה- IP של הרשת. הדרך הפשוטה ביותר לעשות זאת היא באמצעות שליחת Ping ב- broadcast ולכן זה מה שתממשו. כלומר - שלחו Ping ושימרו את כתובות ה-IP מכל המכונות שענו לכם. מכיוון שישנם רכיבים שונים ברשת שעשויים לא להגיב לפינג שכזה, אנחנו נשתמש בנוסף בפרוטוקול המכונה ARP - Address Resolution Protocol אשר בו משתמשת כל יחידה ברשת לשדר פקטות מדי פעם עם פרטים שעשויים להיות רלוונטיים עבור שלב זה. הרכיב שתפתחו יאפשר לשרת התוקף לבקש מיפוי של הרשת הפנימית. מרגע זה המחשב המותקף יתחיל להאזין לפקטות שעוברות ברשת הפנימית ובמקביל ישלח הודעת broadcast. על ידי ניתוח של פקטות ה- ARP והתשובות של ה- ping עליכם להבין מה קורה ברשת הפנימית ולבנות תשובה מסודרת לשרת התוקף הממפה את הרשת הפנימית. על התשובה לכלול את כתובות ה- IP וה- MAC של המחשבים ברשת הפנימית, עם מיפוי בין כתובת IP לכתובת ה-MAC הרלבנטית אליה.

תרגיל 10:

עכשיו כשאנחנו יודעים אילו מחשבים קיימים ברשת הפנימית של המחשב המותקף, אנחנו רוצים שתהיה לנו אפשרות להעביר תעבורה של מחשב ספציפי ברשת הפנימית דרך המחשב המותקף. הדבר יאפשר לנו להאזין לתעבורה של מחשב אחר ברשת (לא המחשב המותקף). זאת נעשה באמצעות מתקפה המכונה ARP Spoofing. עליכם לממש רכיב זה, שבו המחשב המותקף יקבל את כתובת ה- IP וכתובת ה- MAC של המחשב ברשת הפנימית אותו אנחנו מעוניינים לתקוף והמחשב המותקף יבצע את המתקפה. למעשה אנחנו רוצים שהמחשב המותקף לאחר ההתחזות ישמש כ- MITM - man in the middle לתעבורה הזאת. כלומר כל התקשורת בין המחשב החדש שאנחנו תוקפים לבין הנתב,

תעבור דרך המחשב המותקף עליו אנחנו כבר שולטים. שימו לב שמדובר באתגר לא פשוט. מומלץ מאוד להיעזר ב- SCAPY לצורך כך.

* לאלו מכם שרוצים לאתגר את עצמם מעט יותר עליכם לבצע את את מתקפת ה- MITM דו-צדדית. כלומר גם התעבורה מהנתב אל המחשב החדש אותו אנחנו תוקפים תעבור דרך המחשב המותקף עליו אנחנו כבר שולטים.

תרגיל 11:

בכדי שנוכל לעקוב אחר התעבורה ברשת של המחשב המותקף, בין אם לאחר ביצוע ה- ARP Spoofing או מבלי, בשלב זה נבנה רכיב נוסף שבו נוכל לבקש מהמחשב המותקף להעביר לנו את החבילות (פקטות) שעוברות דרכו. בנוסף, עליכם להגדיר פילטר אשר יגדיר איזה סוג חבילות אתם מעוניינים שהמחשב התוקף יעביר לכם. הפילטר יכול להיות על הפרוטוקול, הפורט, כתובות IP ועוד. בעת השימוש ברכיב השרת מגדיר למחשב המותקף לאורך כמה זמן הוא מעוניין שיסניף את התעבורה. ברגע זה יתחיל המחשב המותקף לאסוף את המידע. בעת סיום מקטע הזמן המבוקש, המחשב המותקף צריך להעביר את המידע לשרת התוקף בפורמט pcap.

תרגיל 12:

בשלב זה עליכם לאפשר למחשב התוקף להחליף את השרת שנותן תשובות DNS אצל המחשב המותקף. זהו תהליך המכונה DNS Poisoning. כתובת ה- DNS החדשה תהא זו של השרת התוקף כאשר הוא, השרת, יחליט אילו כתובות IP הוא מחזיר לכל כתובת. עליכם לכלול קובץ DB שכולל עבור כל שם שאתם מחליפים - מיפוי בין השם לבין כתובת ה-IP. שימו לב שעבור כתובות

שלא הגדרתם באופן מפורש ב- DB, תוחזר כתובת ה- IP האמיתית של אותו Domain name. ברגע שהשלמתם את הנ"ל עליכם לבנות אתר שנראה זהה ל-

google ובכל פעם שהמחשב המותקף פונה לגוגל, להציג לו את האתר שלכם. ברגע שמתבצע חיפוש, אתם תשמרו את הערך שחיפש המחשב המותקף בקובץ Txt בשרת ותעבירו את בקשת החיפוש לדף גוגל המקורי. כך המחשב המותקף יקבל את התוצאה האמיתית אך אתם תוכלו לעקוב אחרי כל דבר שהוא חיפש.

בהצלחה!