Übungsdokument WHH3

Dokumentieren Sie Ihre Aktivitäten in Wort und Bild, gehen Sie in Ihrem Dokument davon aus, dass Sie jemanden erklären möchten was Sie tun – d.h. kommentieren Sie auch unbedingt auch Ihren Sourcecode! Bei unklarer bzw. nicht ausreichender Dokumentation gibt es Punkteabzüge!

Erstellen Sie ein Dokument inklusive Deckblatt auf dem auch Ihr Name steht, Inhaltsverzeichnis und eventuell Literaturverzeichnis, sofern Sie auf externe Dokumente (andere als die Vorlesungsfolien) verweisen. Packen Sie das Dokument inklusive aller Files wie z.B. Python Scripte in ein ZIP oder RAR File.

Aufgabe 1 (4P)

Als Sie in der Früh ins Büro kommen ersucht Sie Ihre Kollegin Beate gleich ins Besprechungszimmer zu kommen. Dort erfahren Sie, dass die Forensik Abteilung bei Ihrer Untersuchung eines Sicherheitsvorfalls bei einem Ihrer wichtigsten Kunden festgestellt hat, dass die bislang unbekannte APT Gruppe „No Regerts“ offenbar über einen Social Engineering Angriff Zugriff auf das System erhielt.

Der Kunde hat daraufhin sofort Ihr Red Team beauftragt die User Awareness und Sicherheit im Hinblick auf Social Engineering Angriffe und die vorhandenen Gegenmaßnahmen zu testen. Das Ziel des Red Teams ist es eine mehrstufige, möglichst ausgeklügelte und **überzeugende** Spear Phishing Kampagne auf Executive Mitarbeiter zu starten.

Das Ziel gilt als erreicht, sobald es dem Team gelingt eine Bind Shell auf einem full patched Windows 10 Rechner **mit** eingeschaltetem AMSI zu starten und sich damit zu verbinden.

Aufgabe 2 (2P)

Nachdem die Social Engineering Kampagne ein voller Erfolg war und es Ihrem Team gelungen ist Ncat.exe zur Ausführung zu bringen kam Ihr Kollege aus der Schulungs- und Weiterbildungsabteilung mit einer Bitte zu Ihnen. Dort wurde für ein externes Schulungs- und Ausbildungsprogramm eine Anwendung erstellt, die bewusst Vulnerabilities beinhaltet. Man ersucht Sie nun diese Anwendung zu testen und exploiten, um eine Einschätzung zu bekommen wie herausfordernd die Aufgabe für die Schulungsteilnehmer sei. Wichtig sei, erklärt man Ihnen, dass Sie, sofern Sie in der Lage sind die Anwendung zu hacken unbedingt dies mittels eines Egghunter Exploits machen sollen, egal ob es auch andere Lösungen gäbe, da die Schulung eben dieses Thema behandelt.

Auf Ihre Nachfrage, welche Schulungsrechner verwendet werden meinte der Kollege, es soll ja nicht zu anspruchsvoll sein also 32 Bit Rechner mit deaktivierter DEP und ASLR.

Mit den Worten „endlich wieder ein Zero day“ machen Sie sich sogleich ans Werk.

Aufgabe 3 (6P)

Na so schwer war das wirklich nicht und für Sie natürlich keine Herausforderung. Da man aber bekanntlich nur an diesen wächst, fordern Sie sich gleich selbst heraus!

Sie definieren sich selbst folgende Spielregel, Sie versuchen die Anwendung diesmal ohne Egghunter allerdings mit eingeschaltetem DEP und ALSR zu exploiten. Schaffen Sie das bekommen Sie die volle Punkte Anzahl, schaffen Sie den Exploit nur mit aktiviertem DEP immerhin noch die halbe.

Aufgabe 4 (8P)

Sie staunten nicht schlecht als plötzlich zwei Männer in Anzügen in Ihrem Büro standen, sich als Vertreter einer Regierungsbehörde auswiesen und Sie um Hilfe baten!

Ersten Ermittlungen zufolge nutzt die erfolgreiche APT Gruppe „No Regerts“ die auch für den Angriff auf Ihren Kunden verantwortlich gemacht wird, ein gehacktes Service im Netz um Zugriffspassworte auf einen hochverschlüsselten IRQ Chat auszutauschen. Die darauf angesetzten Spezialisten konnten die verwendete Software inklusive des Sourcecodes recherchieren, darüber hinaus hat man durch Scans und Fingerprinting die Version des Linux Servers erfahren. Alle Versuche das Service selbst zu hacken scheiterten bislang.

Nun wendet man sich hilfesuchen an Sie und hofft, dass Sie Ihrem Ruf gerecht werden und das IRQ Chat Passwort liefern können. Als Sie einwilligen, den Auftrag anzunehmen überreicht man Ihnen einen USB Stick mit den bereits recherchierten Informationen und gibt Ihnen die IP Adresse der Service 10.105.21.174:8080 Neugierig und ein wenig geehrt fühlend beginnen Sie das Service zu analysieren.

Anmerkung:

Das Service ist im FH Netz, verbinden Sie sich mit VPN.

Als Credentials für das Service selbst verwenden Sie beim Login Ihren TW Account sowohl als Login als auch als Password, getrennt durch einen Doppelpunkt. D.h. Eingabe beim Login: zum Beispiel ic16m001:ic16m01

Der Scope ist die Beschaffung des Flags. Alle Aktivitäten, die über diesen Scope hinausgehen z.B. Angriffe auf andere Rechner oder Veränderung bzw. mutwillige Beschädigung des Systems werden nicht geduldet!

Volle Punkteanzahl, wenn Sie ASLR ohne Bruteforce bypassen können, ansonsten nur die halbe!