TH Brandenburg
Online Studiengang IT Sicherheit
Fachbereich Informatik und Medien
Netzwerksicherheit
Prof. Dr. Michael Pilgermann

Einsendeaufgabe 1

Wintersemester 2023

Abgabetermin 8. Oktober 2023

Gruppe 11
Mathias Baumbach (Matr-Nr. 20213703)
Mara Schulke (Matr-Nr. 20215853)

Zusammenfassung

Innerhalb dieser Einsendeaufgabe werden verschiedene Aspekte der Netzwerksicherheit – vor allem aus der Angreiferperspektive – betrachtet. Im Rahmen der Bearbeitung konnten wir wertvolle Erfahrungen sammeln – gerade die Aufgabe 2.5 (Google-Hacking) hat uns erneut vor Augen geführt wie wichtig eine entsprechende Absicherung von IT-Systemen ist, da wir innerhalb von wenigen Minuten vollen Zugriff auf die Datenbank eines PHP Web-Servers erlangen konnten. Wir haben den Betreiber informiert und anonymisiert. So, dass diese Dokumentation nicht zu einer weiteren Ausnutzung verwendet werden kann.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Vorbereitungen

Die bevorzugte Methode zur Beantwortung der Einsendeaufgabe besteht darin, dass Sie entweder ParrotOS oder Kali Linux als virtuelle Maschine auf Ihrem Rechner installieren. Diese beiden Linux-Distributionen sind speziell auf die IT-Sicherheit ausgelegt und haben daher viele interessante Tools schon vorinstalliert. Tipp zur Durchführung: Laden Sie von ParrotOS eine .ova für virtuelle Maschinen herunter (genauer die .ova der Security Edition; Tipp: das Superuser-Password lautet dann "parrotünd nicht "toor"wie bei anderen Versionen). Falls noch nicht vorhanden, installieren Sie Virtualbox und führen die virtuelle Maschine darin aus. Leider gibt es in der letzten Zeit zunehmend Prozessorarchitekturen (gerade für Mac), bei denen keine Möglichkeit zum Betrieb von virtuellen Maschinen besteht. Sollte das der Fall sein, dann bearbeiten Sie die Aufgaben auf Ihrem eigenen Betriebssystem. Sie müssen dafür die Tools einzeln herunterladen.

2 Durchführung

2.1 Telnet und Wireshark

Aufgabenstellung

Wireshark ist bei ParrotOS und Kali Linux vorinstalliert. Es kann ansonsten von der Wireshark-Seite heruntergeladen werden. In der Wireshark-Datei im Kurs (telnet.pcapng) ist eine Aufzeichnung eines Einlog-Vorgangs mit Telnet zu finden. Suchen Sie darin das Passwort.

Antwort

Nach dem wir die Datei analysiert und den Telnet-Loginvorgang

2.2 Schwachstellenscan I

Aufgabenstellung

Verwenden Sie `nmap` (bei ParrotOS und Kali Linux vorinstalliert), um verschiedene Scans des Testservers nwsmooc.mooin.org durchzuführen. Erklären Sie die Ergebnisse, wobei mindestens drei Tests mit jeweils unterschiedlichen Parametern durchgeführt werden müssen. Versuchen Sie dabei u.a. herauszufinden, welche Dienste auf dem Zielserver installiert sind und welches Betriebssystem verwendet wird.

Antwort

2.3 MAC Spoofing

Aufgabenstellung

Ebenfalls bereits bei ParrotOS und Kali schon vorinstalliert ist das Tool `macchanger`. Machen Sie sich mit dessen Möglichkeiten vertraut, wobei z.B. ein Video von HackerSploit nützlich sein kann: `https://www.youtube.com/watch?v=bshXz5r-CQA`. Senden Sie anschließend Datenverkehr mit gefälschter MAC-Adresse und zeichnen diesen mit Wireshark auf. Fertigen Sie geeignete Screenshots mit Erklärungen (wie müsste es richtig sein? wo ist die gefälschte MAC-Adresse in Wireshark zu sehen?) dazu an. Mac- und Linux-Nutzer verwenden für die Aufgabe ebenfalls `macchanger` oder `ifconfig`. Windows-Nutzer schauen sich bitte das Youtube-Tutorial an: `https://www.youtube.com/watch?v=V3Pcc8b_m0U`. Hinweis: Bei der ersten Methode heißt der Eintrag in den erweiterten Einstellungen nicht "Network Address", sondern "Locally Administered Address".

Antwort

2.4 Schwachstellenscan II

Aufgabenstellung

Verwenden Sie das bei ParrotOS und Kali Linux vorinstallierte WPScan (WordPress Vulnerability Scanner) und führen Sie einen Scan von https://nwsmooc.mooin.org durch. Erklären Sie die Ergebnisse.

Hinweise:

- Es ist keine Registrierung beim Anbieter erforderlich. Durch eine Registierung würde man ein Token erhalten, um Schwachstellentests durchführen zu können. So ist die Aufgabe auf eine Informationssammlung beschränkt.
- Bei einem Test mit ParrotOS gab es zunächst eine Fehlermeldung, dass ein Update der Datenbank nicht möglich sei. Ein allgemeines Update (`sudo apt-get update && apt-get upgrade`) konnte dieses Problem beseitigen.

Sollten Sie Mac oder Linux verwenden, dann installieren Sie WPScan direkt von Github. Sollten Sie keine Möglichkeit zur Durchführung dieses Aufgabenteils finden, sprechen Sie die Betreuenden auf eine Ersatzaufgabe an.

Antwort

2.5 Google-Hacking

Aufgabenstellung

Mit "Google Hackingïst gemeint, dass man die Google Suche zum Auffinden von S oftwareinstallationen mit Schwachstellen nutzen kann. Eine Sammlung von Beispielen ist bei `https://www.exploit-db.com/google-hacking-database/` zu finden. Erklären Sie anhand von drei selbstgewählten Beispielen, was man damit herausfinden kann. Achtung: Firefox und Google Chrome warnten teilweise beim Aufruf der Seite und bezeichneten diese als riskant. Man kann die Seite aber aus einem Browser innerhalb von Kali Linux oder ParrotOS aufrufen, dann kommt keine Warnung.

Antwort