Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Cybersecurity - Praktikum

Bachelorstudiengang IT Security
Modul Cybersecurity – Praktikum
Sommersemester 2022

Im Rahmen dieses Praktikums werden ausgewählte Probleme und Fragestellungen aus dem Bereich der Sicherheit von Web-Applications, Passwortschutz und Hardware-Hacks behandelt. Sie kennen nach der Bearbeitung der Aufgaben praktische Aspekte, sowie die (Un-) Sicherheit konkreter Verfahren und Produkte.

Virtuelles Labor

Zur Bearbeitung der Übungen wird in diesem Modul ein virtuelles Labor verwendet. Es basiert auf drei virtualisierten Betriebssystemen. Ein Windows 10 System WINDOWS, eine Linux-Kali-Distribution LINUX und Metasploitable3 METASPLOITABLE. Auf allen Systemen sind die notwendigen Tools für das Praktikum vorinstalliert. Damit können direkt die Übungen bearbeitet werden, ohne dass eine langwierige Einrichtung der Anwendungen erfolgen muss. Beide Systeme sind auf möglichst einfache Bedienung hin optimiert und nicht sicher konfiguriert, daher sollten Sie nicht direkt mit dem Internet verbunden werden.

Windows 10 WINDOWS

Unter „I:\INF\TI\Veranstaltungen\Malik\Virtuelle Maschinen\“ liegt ein angepasstes Windows-System. Dieses können Sie über die Datei „HSAS_WINDOWS.vmx“ mit dem VMWare Player starten. Der Admin-Benutzer hat kein Passwort.

Kali-Linux LINUX

Unter „I:\INF\TI\Veranstaltungen\Malik\Virtuelle Maschinen\“ liegt ein angepasstes Kali Linux-System. Dieses können Sie über die Datei „HSAS_KALI.vmx“ mit dem VMWare Player starten. Das „root“ Passwort lautet „root“.

Metasploitable3 METASPLOITABLE

Unter „I:\INF\TI\Veranstaltungen\Malik\Virtuelle Maschinen\“ liegt ein angepasstes Kali Linux-System. Dieses können Sie über die Datei „HSAS_METASPLOITABLE.vmx“ mit dem VMWare Player starten. Das „vagrant“ Passwort lautet „vagrant“.

Übung 1: Metasploitable3

Nach Bearbeitung dieser Übungsaufgaben kennen Sie typische Sicherheitslücken eines Betriebssystems und können nachvollziehen welche Fehler häufig begangen werden. Sie können Analysemethode anwenden um Sicherheitslücken aufzuspüren und haben so die Möglichkeit die Sicherheitslage zu beurteilen.

Metasploitable3

Metasploitable3 ist eine virtuelle Maschine, die mit einer Vielzahl an Sicherheitslücken erstellt wurde. Sie soll als Ziel für das Testen von Exploits mit Metasploit verwendet werden. Metasploitable3 wird auf Github gehostet, ist somit quelloffen und kann gemeinsam mit der Community weiterentwickelt werden. Es hat einen CTF Modus und verwendet Spielkarten als Flags.

Informationen & Download: https://github.com/rapid7/metasploitable3

Dokumentieren Sie alle Teilaufgaben mit Screenshots für Ihre Abgabe. Die Ausgaben der einzelnen Aufgabenteile werden auch teilweise für darauffolgende Aufgaben benötigt.

Nützliche Links zum Einstieg für diesen Aufgabenteil:
OFFENSIVE SECURITY – METASPLOIT UNLEASHED
KALI LINUX - TOOLS LISTING

Übung 1.1: Information Gathering LINUX

Nmap (Network Mapper) ist ein Tool zum Scannen und Auswerten von Hosts in einem Computernetzwerk (Portscanner).

A) Port-Scan mit NMAP - Subnetz

Lesen Sie die IP-Adresse des Kali-Systems aus und scannen Sie das Subnetz um die IP-Adresse das Metasploitable3 Systems herauszufinden.

B) Scan des Zielsystems (Dienste)

Scannen Sie das Metasploitable3 System mit NMAP. Verwenden Sie dazu die Stealth-Option. Welche Dienste sind aktiv?

C) Scan des Zielsystems (OS)

Scannen Sie das Metasploitable3 System mit NMAP. Verwenden Sie dazu die passende Option um das Ziel-Betriebssystem zu ermitteln.

D) Versionsnummern der Dienste

Führen Sie nun mit NMAP einen aggressiveren Scan durch, um die Versionsnummern der Dienste zu ermitteln. Recherchieren dazu die geeigneten Optionen. Welche Dienste werden nun erkannt?

Übung 1.2: Metasploit Framework LINUX

Das Metasploit Framework ist eine Entwicklungsplattform zum Erstellen und Testen von Sicherheitstools und Exploits.

A) CLI und Exploitsuche

Starten Sie das Metasploit Command Line Interface und durchsuchen (search) Sie die Exploit Datenbank nach Möglichkeiten das System anzugreifen. Nutzen Sie dazu die Liste der Dienste mit ihren Versionsnummern, aus der vorherigen Aufgabe. Wie viele potentielle Exploits haben Sie gefunden?

B) Exploit durchführen

Starten Sie nun den Angriff und führen Sie die mindestens einen Exploit auf einen passenden Dienst durch.
Passen Sie hierzu die benötigten Parameter an (show, set).
Welche Parameter mussten Sie anpassen, dass der Exploit erfolgreich war?

Übung 1.3: Apache Webserver LINUX

Öffnen Sie die URL der Metasploitable3-VM im Browser.

A) Quelltext analysieren

Analysieren Sie den Quelltext der Website. Was ist das Besondere an dieser Website?

B) Login knacken

Analysieren Sie den Login, der bei den Menüpunkten erscheint. Welche Daten werden an den Server gesendet? Wie lauten der Benutzername und das Passwort?

C) Download

Sie haben Ihre erste Flag erhalten. Wie wurde der Download realisiert?

D) CMS Drupal - Analyse

Im Unterordner /drupal ist das Content Mangement System Drupal installiert. Schauen Sie sich die Seiten an. Welche Links zu weiteren Web-Anwendungen können Sie finden? Alternativ kann auch ein Programm wie beispielsweise DirBuster für die Suche von Ordnern/Dateien auf einem Webserver verwendet werden.

E) CMS Drupal - Flag

Dort ist eine weitere Flag versteckt. Finden Sie diese. Wir wurde diese Flag verschleiert?
Tipp: Nutzen Sie das vorinstallierte exiftool.

Übung 1.4: Zweiter Webservice LINUX

A) Fuzzing

Ein weiterer Webservice ist auf dem Port 3500 aktiv. Verden Sie wfuzz und die von Kali bereitgestellten Listen, um nach Unterordner zu suchen.

B) Sicherheitsanalyse

Analysieren Sie nun die gefundenen neuen Unterseiten, dort ist eine Sicherheitslücke vorhanden. Achten Sie vor allem auf die Parameterübergabe. Finden Sie die Zugangsdaten zur MySQL-Datenbank.
Tipp: Können Sie mittels Path Traversal Zugriff auf eine der unter 1.3 D) gefundenen Webanwendungen bekommen?

C) Root Zugriff

Analysieren Sie anschließend weiter die Datenbank. Welche Tabelle mit Zugangsdaten ist besonders interessant? Exportieren Sie die Zugangsdaten in zwei separate Listen. Nutzen Sie das Tool Hydra um diese Zugangsdaten für einen SHH Zugang durchzutesten. Welche Kombinationen sind gültige Logins? Welcher Benutzer hat die Berechtigung root Rechte zu erlangen?

Übung 2: Web Application Security

Nach Bearbeitung dieser Übungsaufgaben kennen Sie typische Sicherheitslücken in Web Applications und verstehen welche Fehler häufig von Web-Entwickler begangen werden. Sie können Analysemethode anwenden um Sicherheitslücken aufzuspüren und haben so die Möglichkeit die Sicherheitslage zu beurteilen.

Cyber Security - Web Demo Plattform

Die Web Demo Plattform für dieses Praktikum, ist bereits im Kali System installiert und unter der IP-Adresse http://127.0.0.1/dp/ erreichbar. Die folgenden Übungen basieren auf den Funktionen der Web Demo Plattform. Sie finden diese unter dem Punkt „Übungen“ entweder im Header der Startseite oder im ersten Kasten der Startseite selbst.

Übung 2.1: Firefox Tools LINUX

Setzen Sie für die Aufgaben die Entwicklerwerkzeuge von Firefox und das Add-on Web Developer ein.

A) Quelltext auslesen

Umgehen bzw. knacken Sie den Passwortschutz, indem Sie den Quelltext auslesen. Wie lautet das Passwort für den Login?

B) Quelltext Analyse

Umgehen Sie den Passwortschutz, indem Sie den Quelltext analysieren. Wie lautet das Klartextpasswort für den Login?

C) URL-Manipulation

Manipulieren Sie die URL um den Passwortschutz zu umgehen. Wie kann hier die URL manipuliert werden, damit Sie als Admin angemeldet sind?

D) Parameter-Manipulation

Um den Passwortschutz zu umgehen, manipulieren Sie die POST-Parameter. Welche Parameter müssen hier manipuliert werden, damit Sie als Admin angemeldet sind?

E) Cross-Site-Scripting (reflected)

Schleusen Sie einen temporären JavaScript-Code in diese Seite ein. Erzeugen Sie zur Bestätigung ein Dialogfenster mit dem Befehl alert(), welches die Meldung „XSS“ ausgibt.

F) Cross-Site-Scripting (persistent)

Schleusen Sie einen JavaScript-Code dauerhaft in diese Seite ein. Erzeugen Sie zur Bestätigung ein Dialogfenster mit dem Befehl alert(), welches die Meldung „XSS“ ausgibt.

G) Session Hijacking - Cookie manipulieren

Manipulieren Sie die vorhandenen Cookie Einträge, damit Sie angemeldet sind. Verwenden Sie dazu die Entwicklerwerkzeuge von Firefox. Setzen Sie die folgende Session-ID: 042fe0176a89aade16edb0e8665db4e9 ein.

H) Session Hijacking - Cookie klauen

Analysieren Sie auf der Demo-Plattform den Login unter „Übungen“ > „6. Session Hijacking - Cookie klauen“. Lesen Sie die vorhandene Cookie Einträge mit JavaScript aus und geben Sie diese zur Bestätigung in einem Dialogfenster mit dem Befehl alert() aus.

I) Session Hijacking - Cookie setzen

Setzen Sie ein neues Cookie mit JavaScript, um den Login zu umgehen. Verwenden Sie dazu den variablen Namen „ub_csc_session“ und die folgende Session-ID: N3JPeTE9RB6Mym5f7j4bjYynjrndq

J) Hash-Wert Datenbank

Analysieren Sie den Quellcode und knacken Sie den Hash-Wert. Verwenden Sie dazu eine Online-Datenbank.

K) SQL-Injection

Umgehen Sie den Login mit einer SQL-Injection, indem Sie mit einem SQL-Code die Passwortabfrage austricksen.

L) Cross-Site-Authentication-Attacke

Schleusen Sie einen JavaScript-Code ein, um die Login-Daten auszulesen. Geben Sie dazu die eingegebenen Daten in einem alert()-Fenster aus.

M) Click-Jacking - JavaScript

Manipulieren Sie die Seite so, dass der Benutzer eine ungewollte Aktion auslöst, sobald er auf den Facebook Button klickt. Verwenden Sie dazu JavaScript. Der Benutzer soll dabei von der Manipulation nichts mitbekommen und die Aktion wie gewohnt ausführen.

N) Click-Jacking – HTML & CSS

Manipulieren Sie die Seite erneut so, dass der Benutzer eine ungewollte Aktion auslöst, sobald er auf den Facebook Button klickt. Verwenden Sie dieses Mal dazu HTML und CSS. Der Benutzer soll ebenfalls von der Manipulation nichts mitbekommen und die Aktion wie gewohnt ausführen.

O) Defacement

Schleusen Sie einen Code ein um die Website komplett zu ändern.

Übung 2.2: Tools einsetzen LINUX

A) Hash knacken

Analysieren Sie den Quellcode und knacken Sie den Hash-Wert. Verwenden Sie dazu das Tool hashcat des Test-Systems.

B) Hash knacken - Salt

Analysieren Sie den Quellcode und lesen sie den Hash-Wert und das Salt aus. Generieren Sie mit dem Salt und den bereits bekannten Passwörtern entsprechende Hashes.

C) Brute-Force Angriff

Knacken Sie den Login durch das Ausprobieren von Passwörtern. Verwenden Sie dazu das Tool hydra eines Kali-Systems.

Übung 3: Hardware-Hacks

Nach Bearbeitung dieser Übungsaufgaben kennen Sie die Funktionsweise des Bad USB Angriffsszenarios und verstehen, welche Gefährdungen dadurch entstehen. Sie können die Entwicklungsumgebung Arduino IDE anwenden und Programme zur Simulation einer Tastatur implementieren.

Bad USB

Bei dem Angriffsszenario Bad USB werden USB-Geräte so manipuliert, dass sie eine andere Funktion als vorgesehen ausführen. Damit kann zum Beispiel ein USB-Stick als Tastatur fungieren und so beliebige Befehle einschleusen.

Um diese Angriffsart nachzuvollziehen, verwende wir in diesem Praktikum das Arduino Entwicklungsboard Teensy 3.2. Der USB-Chip unterstütz die Funktion einer virtuellen Tastatur und somit kann eine automatische Tastatur simuliert werden.

Konfiguration

Sie können für diese Aufgabe das System der Hochschule verwenden, dort ist die Arduino DIE vorinstalliert.
+ Arduino Software öffnen und unter „Werkzeug“ -> Platine „Teensy 3.2 / 3.1“ auswählen
+ Ebenso unter „Werkzeug“ -> USB Type „Keyboard“ und Keyboard Layout „Deutsch“ wählen

Beispiel Script

Auf der offiziellen Seiten finden Sie zahlreiche Tutorials und Beispiele, die Sie ebenfalls verwenden können (https://www.pjrc.com/teensy/teensyduino.html). Die Programmierung selbst erfolgt in C bzw. C++, wobei technische Details wie Header-Dateien weitgehend verborgen werden und umfangreiche Libraries automatisch eingebunden werden. Jedes Script hat den folgenden Aufbau:

```
void setup() {
 // Befehle werden einmal ausgeführt
}

void loop() {
  // Befehle werden unendlich in einer Endlosschleife ausgeführt
}
```

Übung 3.1: Teensy Grundlagen

A) LED (leuchten)

Schreiben Sie ein Script, damit die integrierte LED des Teensy Boards dauerhaft leuchtet.
Hinweis: Die LED können Sie später als Feedback verwenden, um den Fortschritt eines Scriptes anzeigen zu lassen.

B) LED (blinken 1)

Lassen Sie nun die LED blinken und passen Sie anschließend die Pausen an, um die LED in unterschiedliche Frequenzen blinken zu lassen. Verwenden Sie dazu die *delay()*-Funktion.

C) LED (blinken 2)

Lassen Sie nun die LED wieder blinken, verwenden Sie aber dieses Mal eine *Variable* zum Speichern des Zustandes und eine *IF-Abfrage*.

D) LED (morse)

Steuern Sie die integrierte LED des Teensy Boards so, an der die Zeichen „ITS“ gemorst werden.

E) Maus (scrollen)
Schreiben Sie ein Script welches alle 500 ms einen Scroll-Vorgang ausführt.

F) Maus (bewegen)
Erstellen Sie ein Script, welches den Mauszeiger kontinuierlich verschiebt – z.B. im Kreis.

G) Maus (positionieren)
Positionieren Sie den Mauszeiger in der Mitte des Bildschirms.

H) Tastaturausgabe
Geben Sie mit dem Teensy automatisch „Hello World“ aus.

I) Ausführen-Dialog aufrufen
Rufen Sie den Ausführen-Dialog mit der dazugehörigen Tastenkombination auf.

J) Internet Explorer starten
Starten Sie den Internet Explorer oder Edge über den „Ausführen“ Dialog von Windows.

K) Website aufrufen
Starten Sie wieder den Internet Explorer und rufen Sie dabei eine bestimmte (frei wählbare) Website auf.

L) Startseite des Internet Explorers ändern
Ändern Sie dauerhaft die Startseite des Internet Explorers.
Hinweis: Es gibt mehrere Methoden diese Aufgabe zu lösen.

M) Datei herunterladen
Laden Sie eine beliebige Datei über die Eingabeaufforderung/PowerShell herunter.

N) Datei herunterladen und ausführen
Laden Sie eine beliebige ausführbare Datei herunter und führen Sie diese nach dem Download aus.

O) Datei erstellen
Öffnen Sie den Text-Editor, schreiben Sie beliebigen Inhalt hinein und speichern Sie diese Datei ab.

P) Datei erstellen und ausführen
Erstellen Sie eine ausführbare Datei im Editor, speichern Sie diese und führen Sie diese anschließend aus.

Q) Datei suchen und löschen
Erstellen Sie manuell eine Datei, suchen Sie diese und löschen sie.

R) Autostart Objekt hinzufügen
Fügen Sie Ihrem Benutzer ein neues Objekt hinzu, dass automatisch beim Betriebssystemstart gestartet wird.

S) Zeichnen mit der Maus EXKURS
Schreiben Sie ein Programm, dass in Paint das Haus des Nikolaus zeichnet.

T) Fenster verstecken EXKURS
Schieben Sie ein Fenster möglichst weit an den Rand, so dass es fast nicht mehr sichtbar ist.

U) Brute-Force EXKURS
Erstellen Sie ein Programm, welches das Passwort einer ZIP-Datei per Brute-Force-Angriff knacken kann.