more security. usd

HACKER CONTEST

Anmeldeaufgabe

Wintersemester 2024/25

usd HeroLab

Autor	**Matthias Göhring, Tobias Hamann, Tim Wörner**
Datum	**30.09.2024**
Klassifizierung	Öffentlich (V0)

1 Allgemeines

Für die Teilnahme am Hacker Contest steht leider nur eine begrenzte Anzahl Plätze zur Verfügung. Diese werden anhand der folgenden Anmeldeaufgabe verteilt.

In diesem Semester gilt es, vier Challenges zu lösen. Drei der Challenges enthalten Flaggen in dem Format „USD{<string>}“, welche es gilt zu finden.

Die Challenges werden in Form einer Zip-Datei bereitgestellt und können unter folgendem Link mit folgendem Passwort heruntergeladen werden:

https://transfer.usd.de/index.php/s/NNpzNqNSeoJzNFr
Passwort: **G00dLuck&H4ppyHacking:)**

Bei der Bearbeitung der Challenges dürfen beliebige Tools zur Unterstützung eingesetzt werden. Es bietet sich an, eine virtuelle Maschine mit einer Linuxdistribution einzusetzen, die für Hackingtools spezialisiert ist (beispielsweise Kali Linux oder ParrotOS). Auf diesen Distributionen sind viele für die Challenges nützliche Tools bereits vorinstalliert.

2 Aufgabe

Die Aufgabe ist, die vier bereitgestellten Challenges zu lösen und dabei die drei Flaggen zu finden. Zusätzlich zu jeder Challenge – vor allem für die Challenge ohne Flagge – soll eine detaillierte Beschreibung erstellt werden, in der festgehalten wird, wie die Challenge gelöst wurde und welche Tools verwendet wurden.

2.1 Challenge Beschreibungen

Challenge 1
Es wird eine pcap-Datei (challenge.pcap) bereitgestellt. Die Aufgabe besteht darin, den Netzwerkverkehr zu analysieren und die versteckte Flagge zu finden. Die Abgabe soll eine kurze Beschreibung beinhalten, wie die Challenge gelöst wurde.

Challenge 2
Es wird eine Audio-Datei (challenge_embedded.wav) bereitgestellt. Die Aufgabe besteht darin, diese zu analysieren und die versteckte Flagge zu finden. Die Abgabe soll eine kurze Beschreibung beinhalten, wie die Challenge gelöst wurde.

Challenge 3
Es wird eine ausführbare Datei (challenge3) bereitgestellt. Die Aufgabe besteht darin diese Datei zu reverse engineeren um die versteckte Flagge zu finden. Die Abgabe soll eine kurze Beschreibung beinhalten, wie die Challenge gelöst wurde.

Challenge 4
Es wird eine docker-compose Datei mit zusätzlichen Helferdateien bereitgestellt. Mit Hilfe dieser Dateien kann eine Webanwendung unter *http://localhost:5000* gestartet werden. Die Aufgabe besteht darin, die Schwachstelle der Webanwendung zu finden und auszunutzen. Die Abgabe soll eine kurze Beschreibung beinhalten, wie die Challenge gelöst wurde.

2.2 Bearbeitungszeitraum

Der Bearbeitungszeitraum beginnt mit der Veröffentlichung der Aufgabe. Er endet am **17.10.2024 um 23:59 Uhr**. Alle Abgaben, die nach dieser Frist erfolgen, können leider nicht berücksichtigt werden.

2.3 Abgabemodalitäten

Abgaben werden ausschließlich über die folgende URL entgegengenommen:

https://transfer.usd.de/index.php/s/H8QWYrizS8MKLTH
Passwort (notwendig für den Upload): **G00dLuck&H4ppyHacking:)**
Dateiname: **HC-WiSe24_TU_<Nachname>.pdf**

Als Abgabe wird ein Bericht mit allen Informationen im PDF-Format erwartet. Vollständiger Name, die Matrikelnummer und die (Universitäts-)E-Mail-Adresse müssen auf der ersten Seite des PDF-Dokuments vermerkt sein. Die Form fließt in die Bewertung mit ein! Gruppenarbeit oder Gruppenabgaben sind nicht gestattet. Plagiate führen zum Ausschluss aller Beteiligten von der Teilnahme am Hacker Contest.

Aus dem Bericht sollen die gefundenen Flaggen, sowie Details zur Ausnutzung und verwendete Tools hervorgehen.

Bei Fragen bzgl. der Aufgabenstellung bitte eine E-Mail an: hackercontest@usd.de.