more security. usd

HACKER CONTEST

Anmeldeaufgabe

Sommersemester 2024

usd HeroLab

Autor	**Matthias Göhring, Tobias Hamann, Tim Wörner**
Datum	**15.4.2024**
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, eine Challenge aus dem Bereich der Festplattenforensik zu bestehen. Ein gutes Programm zur Bearbeitung der Aufgabe ist Autopsy[1]. Es bietet sich an, Parrot OS zu verwenden. Dort ist Autopsy vor-installiert.

Das Festplattenabbild wird im RAW-Format zur Verfügung gestellt. Es ist, um Bandbreite zu sparen, mit *gzip* gepackt, und muss für den Import in gängige Programme entpackt werden. Es lässt sich unter folgendem Link und Passwort finden:

https://transfer.usd.de/index.php/s/GyifRtKEbB7DpSd
Passwort: **G00dLuck&H4ppyHacking:)**

2 Aufgabe

Die Aufgabe ist die Durchführung einer forensischen Analyse des verlinkten Festplattenabbildes. Die Lösung sollte eine Übersicht über das genaue Vorgehen des Angreifers und einige Tipps zur Absicherung des Systems enthalten. Eine Übersicht der Tools, welche zur Lösung benutzt wurden, soll ebenfalls eingereicht werden.

2.1 Szenario

Eine kleine Firma hat einen IT-Berater angestellt, um Zertifikate für verschiedene Dienste zu generieren. Kaum hat dieser die Arbeit abgeschlossen und das Gebäude verlassen, zeigt das in der Firma verwendete IDS einen Angriff auf den eigens für diesen Zweck eingerichteten Server an.

Besorgt wegen der Sicherheit der erzeugten Zertifikate fordert das Unternehmen eine forensische Untersuchung des Servers an. Zu klären ist die Frage, ob ein Angriff auf das System stattgefunden hat, und wenn ja, welche Daten vom System gestohlen wurden. Alle Informationen, die dabei über den Angreifer gefunden werden können, sind ebenfalls von Bedeutung.

[1] https://www.sleuthkit.org/autopsy/

Der Leiter der Technikabteilung erwartet dabei nicht nur einen abschließenden Bericht über die Daten, sondern wünscht sich darüber hinaus noch eine stichwortartige Liste mit Vorschlägen zur Härtung des Servers. Aufgrund von anderen Projekten soll der Server nicht neu aufgesetzt, sondern weiterbenutzt werden. Ist dies empfehlenswert?

Der Server selbst hat die IP-Adresse **192.168.0.1**. Der Berater hat das Benutzerkonto „*root*“ verwendet und hat entweder direkt an dem Rechner oder von den Adressen **192.168.5.23** und **192.168.23.5** gearbeitet. Ansonsten sollte niemand Zugriff zu dem Rechner bekommen haben.
Der Berater hat den Rechner morgens aufgesetzt und die Zertifikate erzeugt. Er hat direkt im Anschluss das Haus verlassen. Kurz darauf hat das IDS-System den Angriff gemeldet.

2.2 Bearbeitungszeitraum

Der Bearbeitungszeitraum beginnt mit der Veröffentlichung der Aufgabe. Er endet am **02.05.2024 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/zJXoGf9RK8o9X98
Passwort (notwendig für den Upload): **G00dLuck&H4ppyHacking:)**
Dateiname: **HC-SoSe24_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 Angriffsdetails und Schwachstellen hervorgehen. Hierfür ist eine Aufzählung in Form von Stichpunkten ausreichend (z.B. „root-Passwort zu schwach und durch Wörterbuchangriff zu erraten“).

Mindestangaben des Berichtes:

- Sollten die Zertifikate noch benutzt werden?
- Darf das System weiterverwendet werden?

- Wenn ein Angriff stattgefunden hat:
  - Wie ist der Angreifer auf das System gekommen?
  - Was hat der Angreifer auf dem System gemacht?
  - Was ist durchzuführen, um das System abzusichern?
  - Welche Details könnt Ihr über den Angreifer selbst aus dem Image extrahieren?

Zusätzlich könnten folgende Fragen im Bericht beantwortet werden.

- Wie wird die Konfiguration des Servers beurteilt?
- Wie ist die vom Berater geschriebene Software zu beurteilen?
- Sollte eine CA in dieser Weise betrieben werden?

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