Vorlesung Python Hacking 2022
Aufgabenstellung der Hausarbeit

Es soll eine Software mit einer unten beschriebenen „Schadwirkung“ und einem nicht ganz offensichtlichen Code entwickelt werden.

1. Einige Regeln

- Die Hausarbeit ist eine individuell erbrachte Leistung. Falls eine Arbeit in Gemeinschaft erbracht wird, steigt das erwartete Ergebnis entsprechend und die Anteile müssen in Form einer Verantwortlichkeitsmatrix (RACI-Matrix[1]) dargestellt werden.
- Die eigene Arbeit darf selbstverständlich andere Arbeiten verwenden, muss diese aber vollständig zitieren.
- Die Arbeit muss einen kreativen Eigenanteil enthalten.

2. Fachliche Vorgaben

Die Software soll auf einem Opferrechner mit MS-Windows-Betriebssystem oder mit Linux-Betriebssystem ausführbar sein.
Die Software soll in Python (als .exe) entwickelt werden.

Folgende Funktionalitäten sollen enthalten sein

1. Opfer-Server:

- Der Opfer-Server soll ein http-Server sein (z. B. Apache).
- Auf dem Server soll eine Site mit angemessener Komplexität eingerichtet werden. So sollen mehrere Verzeichnisse vorliegen, in denen verschiedene Inhalte abgelegt sind (z. B. .html, .jpg, .css), die in HTML-Seiten integriert sind. Ein Teil der Inhalte soll von außen nicht durch Verlinkungen erreichbar sein (z. B. ein isoliertes Verzeichnis mit vertraulichen Daten)
- Denkbare Funktionalitäten könnten ein kleiner Shop oder ein WordPress-Blog sein.
- Zur Wartung des Servers sollen eine Admin-Schnittstellen eingerichtet sein, wie z. B. ssh und ftp. Die Zugänge sollen mit einer (angreifbaren) Authentifikation versehen sein.

2. Angriffe auf den Opfer-Server

2.1. Ein Spider-Angriff soll versuchen alle Inhalte des Servers aufzuspüren und herunter zu laden.

2.2. Ein automatisierter Browser-Zugriff per Selenium o.ä. soll versuchen alle Seiten zu besuchen und z. B. Bestellungen oder dergleichen zu veranlassen

[1] https://de.wikipedia.org/wiki/RACI

2.3. Ein Angriff auf die Administrationszugänge per Wörterbuch-Angriff soll die Zugangsdaten erlangen.

2.4. Mit den Zugangsdaten soll eine Schadsoftware (SW) auf den Opfer-Server geladen werden können die dort ausgeführt wird. SW soll ein Defacement auf der Site umsetzen sowie die Zugangsdaten ändern. Zudem sollen mittels SW Daten, die von außen nicht zugänglich sind, auf einen entfernten Rechner geladen werden.

3. Weitere Merkmale

- Die Übertragung der gestohlenen Daten soll möglichst unauffällig in Form von Daten-Exfiltration umgesetzt werden. Dazu kommen als Transportmittel z.B. DNS-Records, Cookies oder Tweets in Frage.
- Folgende Maßnahmen sind zu treffen, damit der Code von SW nicht ganz trivial analysiert werden kann:
  - Es dürfen keine Passwörter, Schlüssel IP-Adressen, URLs oder dergleichen im Klartext zu erkennen sein.
  - Das Debugging soll erschwert werden.
  - Es sind mehrere übliche Methoden der Code Obfuskation zu verwenden
- Netzwerkverbindungen arbeitet mit Transportverschlüsselung.

4. Optional Merkmale:

- Optional soll SW über Netzwerk in seiner Ausführung per Reverse Shell vom Server steuerbar sein
- Optional verwendet SW einen Packer.
- Optional verwendet SW Methoden, die die Ausführung in einer virtuellen Maschinebehindern.
- Optional erkennt SW„feindliche Prozesse“ und reagiert darauf adäquat (exit oder schlafen oder andere unauffällige Aktion)
- Optional verwendet SW Methoden der Rechteausweitung auf dem Server.

Nach Absprache dürfen Abweichungen in der Funktionalität vorgenommen werden.

5. Abgabe und Abnahme

Es ist eine Dokumentation abzugeben, welche den Entwurfsvorgang, die Implementierung und den Programmablauf ausführlich genug beschreibt, abzugeben. Der Umfang der Dokumentation kann beispielsweise fünf bis zehn Seiten (ohne Listings) betragen.
Der Quellcode (am besten als Projekt organisiert) und der ausführbare Code sind ebenfalls abzugeben.
Sie finden in ILIAS unter
https://elearning.hs-albsig.de/goto.php?target=fold_387634&client_id=HSALBSIG
die Abgabemöglichkeit zur Hausarbeit. Spätester Abgabezeitpunkt ist der 27. Jun 2022, 23:55.

Die Abnahme ist am 29.06. zwischen 11.30 Uhr und 14.00 Uhr. Nach der Abgabe werden Zeitschlitze zugeteilt. Die Abnahme ist hybrid im Raum 210-010 und in Webex unter dem Vorlesungslink.
Zur Abnahme wird eine kleine Präsentation erwartet. Die Länge des Vortrags inklusive Vorführung und Befragung sollte 20 Min. nicht überschreiten.