SecLab

Praktikum IT-Sicherheit

- Versuchshandbuch -

Aufgaben

Footprinting

Footprinting stellt bei Sicherheitstests oder vor einem Angriff die Phase der Informationsbeschaffung dar, durch die IP-Adressen, Hostnamen, DNS-Einträge und vieles mehr in Erfahrung gebracht werden sollen. In diesem Versuch werden einige Onlinequellen angezapft, um gezielt solche Informationen über ein Unternehmen zu erhalten.

B.Sc. AI, WI
M.Sc. AI
M.Sc. EB

IT-Sicherheit

Einleitung

Das Internet stellt einen globalen Raum des Informationsaustausches dar, in dem Nutzer durch ihre scheinbare Anonymität, leichtsinniger mit Informationen umgehen als in der Realität. Administratoren geben z.B. sensible Daten über die IT-Infrastruktur ihres Unternehmens preis, ohne an mögliche Folgen zu denken. Bei Problemlösungen werden Internetforen, das Usenet oder andere Plattformen herangezogen, auf denen zum Teil ganze Konfigurationen veröffentlicht werden. Auch bei der Registrierung einer Internetdomain werden Daten verlangt, die später öffentlich verfügbar sind.

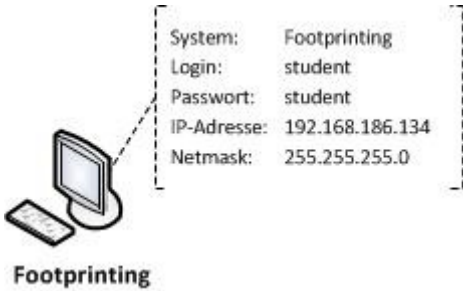
Durch all diese Informationen sind Rückschlüsse auf die Positionen von Angestellten in einem Unternehmen, auf die Vergabepolitik von IP-Adressen oder auf die eingesetzte Software möglich. Dies zeigt, dass von vielen Unternehmen wichtige Daten im Internet öffentlich verfügbar sind und nur nach ihnen gesucht werden muss.

Nachdem eine intensive Datensammlung betrieben wurde, kann in einem nächsten Schritt eine direkte Interaktion mit den gefundenen Systemen beginnen, um diese z.B. auf mögliche Schwachstellen hin zu untersuchen, die dann zur Kompromittierung der Systeme ausgenutzt werden können.

Zugangsdaten

- System: Debian GNU/Linux
- Benutzername: student
- Passwort: student

Netzwerkplan



Wichtiger Hinweis

Ein Großteil der in diesem Versuch gestellten Aufgaben benötigt einen internetfähigen Computer. Da innerhalb der virtuellen Maschinen des SecLab kein Zugriff auf das Internet möglich ist, müssen diese Aufgabenteile auf Ihrem Computer durchgeführt werden. Für eine erfolgreiche Aufgabenbearbeitung wird eine Internetverbindung und ein Webbrowser vorausgesetzt.

Alle Aufgaben, die einen Internetzugang benötigen und somit außerhalb der virtuellen Maschinen des SebLab durchzuführen sind, werden im Folgenden durch das Wort **INTERNET** gekennzeichnet.

Aufgabe 1: Suchmaschinen (Google) (INTERNET)

Für diese Aufgabe verwenden Sie bitte einen beliebigen Webbrowser auf Ihrem Computer.

Eine wichtige Informationsquelle im Internet stellen Suchmaschinen dar, die meist schnell und effizient die gesuchte Antwort liefern. Aus diesem Grund ist es interessant, Suchmaschinen als erste Quelle heranzuziehen und die Suche mit bestimmten Parametern zu optimieren.

a) Erläutern Sie, wie der nachfolgende Suchbefehl von Google interpretiert wird bzw. was bei dieser Suche berücksichtigt wird: *+"hs-fulda" +rz inurl:informatik +filetype:txt*

.....

.....

.....

.....

.....

b) Versuchen Sie mit Hilfe von Google Servernamen und IP-Adressen der Hochschule Fulda in Erfahrung zu bringen. Verwenden Sie dabei gezielt die in der Vorbereitung erwähnte Syntax von Google-Anfragen und notieren Sie Ihre Ergebnisse.

.....

.....

.....

.....

.....

Aufgabe 2: Usenet (Google) (INTERNET)

Für diese Aufgabe verwenden Sie bitte einen beliebigen Webbrowser auf Ihrem Computer.

Neben der Suche auf Webseiten bietet Google die Möglichkeit, über Google-Groups das Usenet zu durchsuchen. Das Usenet ist wie Foren eine wichtige Quelle zum Informationsaustausch und wird gerne bei Problemlösungen herangezogen.

a) Welche Keywörter stehen in Google-Groups zur Verfügung, um die Suche zu optimieren? (Hinweis: Schauen Sie sich die erweiterte Suche und die Hilfe zu Google-Groups an).

.....

.....

.....

.....

b) Versuchen Sie über Google-Groups, unter Verwendung der in Aufgabe a gefundenen Keywörter, weitere Server bzw. IP-Adressen der Hochschule Fulda in Erfahrung zu bringen und schreiben Sie diese auf.

.....

.....

.....

.....

Aufgabe 3: Auswertung des Quelltextes einer Webseite

Führen Sie diese Aufgabe in der virtuellen Maschine des SecLab durch.

Im Quelltext einer Webseite finden sich oft interessante Informationen wieder, die eigentlich nicht für die Öffentlichkeit zugänglich sein sollten. Bei der Entwicklung einer Webseite wird meist nur die fertige Webseite betrachtet und die eingebetteten Kommentare geraten in Vergessenheit. Genau diese Kommentare sind im Folgenden Gegenstand der Betrachtung.

a) Laden Sie die Webseite, die unter der URL *www.test.test* in der virtuellen Maschine verfügbar ist, mit dem Tool *wget* herunter. Verwenden Sie dabei die im Vorbereitungsblatt genannten Optionen.

- Öffnen Sie das Terminal auf dem Desktop der virtuellen Maschine
- Sie befinden sich in Ihrem Home-Verzeichnis
- Wechseln Sie in den Unterordner „Webseite" (*cd Webseite*)
- Verwenden Sie wget zum Herunterladen der Webseite
  (Bsp.: *wget -r -l1 http://www.test.test*)

b) Aus wie vielen Einzelseiten besteht die gesamte Webseite und welcher Befehl wurde zum Herunterladen verwendet?

.....

.....

.....

.....

c) Führen Sie nun eine Kommentarsuche über alle heruntergeladenen Seiten durch. Benutzen Sie dazu die Befehle *find* oder *grep* unter Verwendung von regulären Ausdrücken. Wenden Sie den Befehl auf alle HTML-Dateien im Verzeichnis „Webseite" an.

.....

.....

.....

.....

.....

Aufgabe 4: Whois und Host (INTERNET)

Für diese Aufgabe verwenden Sie bitte einen beliebigen Webbrowser auf Ihrem Computer.

a) Finden Sie über die Webseite *www.whois.net* den Inhaber der Domain *www.hs-fulda.de* heraus. Notieren Sie sich dessen Namen und Kontaktdaten, die in einem möglichen nächsten Schritt für Social-Engineering genutzt werden könnten.

.....

.....

.....

.....

.....

.....

b) Wurden bei der Registrierung der Domain *www.hs-fulda.de* mögliche zuständige Nameserver hinterlegt, die im Netzwerk der Hochschule Fulda untergebracht sind? Ist dies der Fall, so notieren Sie sich deren vollständige Hostnamen und IP-Adressen.

.....

.....

.....

.....

Aufgabe 5: E-Mail Header

Führen Sie diese Aufgabe in der virtuellen Maschine des SecLab durch.

Wenn eine E-Mail versandt wird, wird sie auf ihrem Weg vom Sender zum Empfänger von mehreren Zwischenstationen weitergeleitet. Diese Sprünge werden als „Received:" im eMail-Header vermerkt. Im Folgenden wird der eMail-Header einer System2Teach eMail der Hochschule Fulda genauer analysiert, um die Hostnamen der Mailserver zu erhalten.

Viele eMail-Programme bieten dem Anwender die Möglichkeit, den eMail-Header einzusehen. An dieser Stelle wurde jedoch bereits ein eMail-Header aus einer eMail extrahiert und ist in der virtuellen Maschine verfügbar. Er ist in der Datei „email.txt" enthalten, die sich direkt auf dem Desktop befindet.

a) Notieren Sie die Zwischenstationen in der Reihenfolge, in der die E-Mail über diese geleitet wurde.

.....

.....

.....

.....

.....

.....

Aufgabe 6: archive.org (INTERNET)

Für diese Aufgabe verwenden Sie bitte einen beliebigen Webbrowser auf Ihrem Computer.

Die Webseite *archive.org* führt Speicherungen von Momentaufnahmen digitaler Daten durch, zu denen Webseiten, aber auch Usenet-Beiträge zählen. Es besteht somit die Möglichkeit, einen Snapshot einer Webseite aus der Vergangenheit einzusehen, um so an interessante Daten zu gelangen, die möglicherweise beim Erstellungszeitpunkt des Snapshots im Internet verfügbar waren.

a) Begeben Sie sich auf die Webseite *archive.org* und suchen Sie über „Take Me Back" nach einem Snapshot der Domain *www.hs-fulda.de*.

b) Finden Sie über ältere Snapshots die Domain heraus, unter der die Webseite in der Vergangenheit erreichbar war und notieren Sie sich diese.

.....

.....

.....

.....

c) Ist die „alte" Domain der Hochschule Fulda noch erreichbar und auch auf die Hochschule Fulda registriert? Prüfen Sie die Erreichbarkeit mit Hilfe eines Webbrowsers und die Registrierung über die Webseite *www.whois.net*.

.....

.....

.....

.....

.....