

Übung, Teil 4: **Computer Forensics: Hacked Linux Image**

Typ: 2er Gruppen

Deadline Bericht: 31.12.2005

Abgabegespräch: 31.01.2006

Inhalt

In diesem Teil der Übung soll ein bereitgestelltes, gehacktes Linux-Image untersucht werden.

Das Image steht als VMware Image zum Download bereit. VMware emuliert einen Computer in Ihrem Computer, wodurch Ihr System unangetastet bleibt. Außerdem können Sie sich auf diese Weise einfach eine perfekte Sicherheitskopie des originalen Images anlegen, bevor Sie daran experimentieren.

Umfang

Es gibt 15 Punkte zu erreichen, der Arbeitsaufwand sollte diesen gerecht werden, d.h. circa 7,5 Arbeitstunden pro Person. Dies ist durch Dokumentation der Tätigkeiten zu belegen.

Aufgabenstellung:

- Angabe beachten (siehe unten).
- Downloaden und Installieren von VMware <http://www.vmware.com/download/> (VMware Workstation oder Player).
- Downloaden des Linux Images von der Homepage der LVA (Achtung, >100MB)
- Am besten gleich eine Sicherheitskopie davon anlegen
- Starten des Images in VMware und Durchführung einer forensischen Analyse

Deliverables

- Bericht über die durchgeführte Untersuchung mit detaillierter und übersichtlicher Darstellung der Ergebnisse.
 - Versuchen Sie, den zeitlichen Ablauf in das Dokument zu integrieren; wann ist was passiert?
 - Heben Sie eingegebene Befehle und Listings eindeutig vom übrigen Text ab.
 - Schreiben Sie immer, was sich aus Ihren Resultaten ergibt, was sie bedeuten. Interpretieren Sie Ihren Befund; Befehle und Listings alleine sagen nichts aus.
 - Gewichten Sie Ihre Aussagen: was ist fundiert, was Spekulation?
- Liste aller zusätzlichen verwendeten Programme.

Ablauf:

Dokument- und Abgabebrieflinien beachten! Abgabeformat: PDF

Bewertung

- **Insgesamt 15 Punkte zu erreichen**

Angabe

An einem kalten Wintertag erreicht Sie folgender Auftrag per E-Mail:

User: HowlingWolf
Subject: Hilfe, mein Server wurde gehackt!?

Msg: Hi Leute!
Hoffe ihr könnt mir helfen.
Habe mich heute seit langem wieder mal auf meiner Test-Kiste eingeloggt um mal nach dem Rechten zu sehen. Ok dachte ich mir, sehen wir uns mal Tripwire näher an.
Und was seh ich? Irgendwer hat da was herumgewerkelt und ich wars nicht.
Nun meine Bitte:

Könnt ihr mir helfen herauszufinden, was da wirklich passiert ist und wie bei mir eingebrochen wurde?
Bin nämlich nicht so der Über-Checker, wenns um Forensics geht, aber vielleicht findet ihr ja was.
Ach ja für die Analyse könnten Login / Passwort von nöten sein:

Login: root
PW: HackMePls

Wär super wenn ihr was finden würdet (rootkits, usw.), wär halt toll zu wissen, was der Typ auf meinem Rechner aufgeführt hat.

Ig
Wolf

Helfen Sie dem Auftraggeber HowlingWolf, indem Sie eine forensische Analyse durchführen:

- Versuchen Sie herauszufinden, wie der Angreifer eindringen konnte.
- Welches Sicherheitsloch hat er ausgenutzt?
- Welche Spuren hat er dabei hinterlassen?
- Was wurde am System verändert?
- Wurde ein Rootkit installiert? Wenn ja, wahrscheinlich welches?
- Welche Sicherheitslöcher bestehen?
- Versuchen Sie möglichst viel Information zu sammeln, was wann wie (und am besten auch warum) am System gemacht wurde. Versuchen Sie, die Dinge in einen Kontext und eine zeitliche Abfolge zu bringen (gehen Sie davon aus, dass die Systemuhr nicht manipuliert wurde).

- Verwenden Sie verschiedene in den Folien vorgestellte Tools und dokumentieren Sie Ihren Erfolg.

Tips

- Sie können mit VMware ein .iso Image direkt als CD Laufwerk mounten (dazu muss die Virtual Machine sich im STOP Zustand befinden). So sollten Sie in der Lage sein, z.B. **Helix**, **Auditor Security Collection**, **Whax**, **Whoppix**, **F.I.R.E.**, usw. als bootable CD zu mounten. *Die meisten dieser Distros* enthalten unter anderem auch **The Sleuth Kit** und die ergänzende Oberfläche **Autopsy** (<http://www.sleuthkit.org/>). Durch diese Art des Zugriffs verändern Sie das System nicht.
- Sie können aus VMware heraus auch aufs Internet zugreifen, verwenden Sie `wget`, um eventuelle zusätzliche Software herunter zu laden (bedenken Sie immer, wenn Sie etwas am System ändern, dass sie damit Originaldaten überschreiben, was in einem „echten“ Fall nicht passieren sollte).
- Wenn Sie sich Dateien z.B. mit `ls` auflisten lassen, vergessen Sie nicht, sich auch die unsichtbaren anzeigen zu lassen.
- **ACHTUNG:** der Auftraggeber hat vor dem Angriff sicherheitshalber *Tripwire* installiert (<http://www.tripwire.org/>). Benutzen Sie das Programm, bevor Sie etwas System verändern, ansonsten könnten Ihre eigenen Änderungen gemeldet werden.

Links

<i>Helix</i>	http://www.e-fense.com/helix/
<i>Auditor</i>	http://www.remote-exploit.org/index.php/Auditor_main
<i>Whax</i>	http://www.iwhax.net
<i>F.I.R.E</i>	http://fire.dmzs.com/?section=main