Script-Kiddie

Laborufgabe Block 2

25HS

1 Aufgabenstellung

Auf Vulnhub gibt es sehr schöne VMs sehr schöne, absichtlich verwundbare VMs zum trainieren. Eine besonders vulnerable VM, die für Anfänger geeignet ist finden Sie im Labor //share.cyberlab.fhnw.ch/public/documents/CyslAufgabe1/nullbyte.ova (natürlich nur wenn Sie mit dem CyberLab-Netzwerk verbunden sind). Installieren Sie diese VM auf Ihrer Basisstation und dazu ein Kali-Linux auf einer zweiten VM.

Kali-Linux ist eine spezielle Linux-Distribution, die für Pentester hergestellt wurde und erfreut sich in diesen Kreisen grosser Beliebtheit.

Am besten verbinden Sie die zwei mit einem "Host-only-Netzwerk". Versuchen Sie anschliessend die Flag-Datei im Verzeichnis des Root-Benutzers zu erhalten.

- Sie suchen zuerst die offenen Ports der VM.
- Auf dem gefundenen Webserver suchen Sie nach installierten Seiten an bestimmten Orten.
- Sie extrahieren von gefundenen Grafiken die Exif-Daten.
- Sie brute-forcen einen simplen Passworthash mit einem Wörterbuch.
- Sie machen eine SQL-Injection.
- Sie loggen ein auf dem "nicht-standard-Port" von SSH
- Sie nutzen ein schwaches Schellskript aus.
- ... und natürlich holen Sie sich das Flagfile.

Wenn Sie noch nie so etwas gemacht haben, dann empfiehlt es sich den Walkthrough weiter unten zu Rate zu ziehen.

2 Hilfestellungen

- Das Default Passwort für den Benutzer "kali" auf Kali-Linux ist "Kali"
- Nehmen Sie einen Walktrhough zu Hilfe (z.B. `https://www.nuharborsecurity.com/blog/nullbyte-1-walkthrough`) `https://community.icinga.com/t/how-to-write-a-bash-script-wrapper-newbie-script-for-itl-check-yum-plugin/119`