

Praktikum Systemadministration

Aufgabenblatt 11

Sicherheit

Unterziehen Sie alle Ihre Team-VMs einer Sicherheitsüberprüfung. Identifizieren und schließen Sie nach Möglichkeit alle Sicherheitslücken, die sich im Laufe des Praktikums bisher eingeschlichen haben.

Unter einer Sicherheitslücke sind dabei alle Möglichkeiten zu verstehen, die es bei Zugriff über das Netzwerk oder über einen lokalen Benutzer ermöglichen Rechte oder Informationen zu erlangen, die so vom Administrator nicht vorgesehen waren. Dazu gehören auch z.B. schlechte Passwörter, falsche oder zu großzügige Rechte auf Dateien bzw. Verzeichnissen, fehlende Sicherheitsupdates, unverschlüsselter Austausch von Daten über das Netzwerk und vieles mehr.

Suchen Sie auch auf den VMs der anderen Teams nach Sicherheitslücken. Nutzen Sie dabei die Ihnen zur Verfügung stehenden Ressourcen (z.B. Ihren Account auf den VMs der anderen Teams).

Schützen Sie gleichzeitig Ihre VMs durch die Installation von Programmen zur Feststellung von Angriffen (intrusion detection) sowie durch die Aktivierung eventuell bereits vorhandener Sicherheitsmechanismen ihres Betriebssystems.

Werkzeuge

Es gibt zahlreiche Programme, die Sie bei einer Sicherheitsüberprüfung unterstützen (eine kleine Auswahl):

- nmap
- OpenVAS
- Argus
- Metasploit
- John the Ripper
- Rootkit Hunter

Weitere Informationen finden Sie z.B. auf www.dmoz.org unter *Computers* → *Security* und natürlich mit einer geeigneten Suche bei Google.

Beurteilen Sie jedes der von Ihnen eingesetzten Werkzeuge nach seiner Wirksamkeit und dokumentieren Sie gefundene Sicherheitslücken und wie sie geschlossen wurden in den folgenden Kategorien:

- Eigene VMs, local exploit
- Eigene VMs, remote exploit
- Andere VMs, local exploit
- Andere VMs, remote exploit

Dokumentation

Kopieren Sie alle erzeugten oder veränderten Konfigurationsdateien und ggf. eine Liste der Kommandos (inklusive Aufrufparameter), die bei der Bearbeitung dieser Aufgabe eine wesentliche Rolle gespielt haben, auf den Praktikumsserver in das Verzeichnis:

`psa.in.tum.de:/opt/psa/doc/Team_##/Aufgabe_11/`

und/oder Dokumentieren Sie Ihre Lösung nachvollziehbar im Wiki unter

<https://wiki.rbg.tum.de/Informatik/RBG/PSA/WiSe1617DokumentationderAufgaben>