MNM
TEAM
Munich Network Management Team

Ludwig-Maximilians-Universität München
und Technische Universität München
Prof. Dr. H.-G. Hegering

Praktikum IT-Sicherheit
Übungsblatt 02

6. Scanner und Passwortcracker

(a) Installieren Sie `nmap`, `nessus`, `nikto`[1] und `John the Ripper`[2] entweder als SuSE Paket (wenn vorhanden) oder durch Kompilieren des Quellcodes. Die Tools sind entweder auf der SuSE DVD in `/dev/hdc/` enthalten oder im Internet unter den angegebenen Adressen verfügbar.

(b) Scannen Sie mittels `nmap (man nmap)` die IP-Adress(bereich)e `192.168.216.253`, `192.168.216.128/25` und sich selbst:

i. ohne Optionen
ii. mit einem Fingerprint
iii. Port 20 bis 1000
iv. mit einem FIN Scan

und vergleichen Sie die System-Logdatei-Einträge in `/var/log/...` des Ziel-Systems mit den Shell-Ausgaben von `nmap`. Was ist festzustellen und wie ist das zu interpretieren?

(c) Aktivieren Sie bei Nessus alle Plugins außer "Denial of Service" und scannen Sie sich selbst. Speichern Sie den erzeugten Report ab. Wie ist das Ergbnis zu interpretieren?

(d) Scannen Sie mit Nikto den Webserver auf dem Rechner `test4all`.

(e) Legen Sie auf Ihrer Maschine drei Dummy User mit unterschiedlich schwierigen Passwörtern an. Versuchen Sie anschließend die Passwörter aller im System vorhandenen User zu knacken. Verwenden Sie hierzu den Passwort Cracker John the Ripper. Wie geht der Cracker vor und welche Passwörter konnten geknackt werden? Wie lange hat er jeweils gebraucht? Welche Passwörter sollte man somit nicht verwenden? Was lässt sich über die Beschaffenheit von guten Passwörtern sagen? Vergessen Sie nicht, die Dummy User nach Abschluss der Übung wieder zu entfernen.

7. Rootkit

Auf dem Rechner `hacktest` (`192.168.216.252`) ist ein Rootkit installiert. Auf dem Rechner können Sie sich mit dem Benutzer `secpgast`, Passwort `secp` einloggen, das `root`-Passwort lautet ebenfalls `secp` .

(a) Versuchen Sie, das Rootkit zu entdecken und soviele Informationen wie möglich über das Rootkit zu sammeln (dazugehörige Dateien, Prozesse, Backdoors, gesammelte Informationen).

(b) Wie haben Sie den Rechner untersucht?

(c) Was würden Sie als Reaktion auf das entdeckte Rootkit vorschlagen?

Sie können auf dem Rechner `hacktest` zur Lösung der Aufgaben beliebige Programme installieren und den Rechner nach Ihren Vorstellungen untersuchen. Sollten Sie das Rootkit entdecken verändern Sie es nicht, damit Ihre Kollegen noch was zu suchen haben. Sprechen Sie sich ggf. mit anderen auf dem Rechner eingeloggten Anwendern ab, bevor Sie den Rechner z.B. neu starten oder Software installieren.

8. DoS-Werkzeuge

(a) Beschäftigen Sie sich mit drei der in der Vorlesung vorgestellten DoS-Werkzeugen. Kompilieren sie diese und versuchen Sie, die beschriebene Attacke durchzuführen.

(b) Zeichnen Sie die von den Werkzeugen generierten Datenpakete auf und interpretieren diese.

[1] http://www.cirt.net/code/nikto.shtml
[2] http://www.openwall.com/john/