2.7 Praktische Aufgaben

2.7.1 Scanner und Passwortcracker

1. Installieren Sie `nmap`, `nessus`, `whisker` und `crack` entweder als SuSE Paket (wenn vorhanden) oder durch Kompilieren des Quellcodes. Eventuell muß dazu noch das Kommando `make` im `YaST` installiert werden.

2. Scannen Sie mittels `nmap` die `192.168.216.253` , `192.168.216.128/26` und sich selbst:

   (a) ohne Optionen

   (b) mit einem Fingerprint

   (c) Port 20 bis 1000

   (d) mit einem FIN Scan

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

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

4. Machen Sie mit Whisker einen HEAD und einen GET Scan Ihrer Maschine und vergleichen Sie die Logfileeinträge.

5. Legen Sie auf Ihrer Maschine drei Dummy User mit unterschiedlich schwierigen Passwörtern an. Erzeugen Sie aus der `/etc/passwd` und `/etc/shadow` das Inputfile und lassen Sie den Passwortcracker Crack5.0 laufen. Wie lange hat der Cracker gebraucht? Was läßt sich somit über die Beschaffenheit von Passwörtern sagen?

2.7.2 Rootkit

Auf dem Rechner `hacktest` (`192.168.216.252`) ist ein Rootkit installiert. Auf dem Rechner können Sie sich mit dem Benutzer `secpgast`, Passwort `pcsec` einloggen, das `root`-Passwort lautet `y;x:c_v,b.n-` .

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

2. Wie haben Sie den Rechner untersucht?

3. 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.

2.7.3 DoS-Werkzeuge

1. Beschäftigen Sie sich mit drei der vorgestellten Programme. Kompilieren sie diese und versuchen Sie, die beschriebene Attacke durchzuführen.

2. Zeichnen Sie die von den Werkzeugen generierten Datenpakete auf und interpretieren diese.