Aufgabe 3.1: Worauf noch zu achten wäre!

Im Rahmen der bisherigen Aufgabenblätter haben Sie schon einiges abgesichert, aber es haben sich auch Fehler und Lücken eingeschlichen. Überprüfen Sie unbedingt:

- Haben Sie den Zugriff auf die Netzwerk-Firewalls selbst auch minimal gehalten? Oder ist nur die Queue FORWARD konfiguriert?
- Haben Sie Pakete verboten, die nicht IPv4 sind? Das betrifft sowohl IPv6-Pakete als auch andere Netzwerk-Protokolle als IP (oft nicht mehr relevant, aber das heißt ja nicht, das ein Angreifer das nicht ausnutzen könnte)

Aufgabe 3.2: Host-Firewalls

Da wir keine zwei unterschiedlichen Firewall-Produkte einsetzen können/wollen, sichern wir uns mit Host-Firewalls etwas besser ab. Auch wenn wir das gleiche Produkt (iptables) einsetzen, und somit Implementierungsfehler in dem Produkt sowohl auf der Netzwerk- als auch auf den Host-Firewalls vorliegen würden, schützt es tatsächlich vor Angriffen von als „vertrauenswürdig“ eingestuften Rechnern. Wird ein DMZ-Server über einen angreifbaren Dienst kompromittiert, würde dieser Rechner vermutlich nach anderen Rechnern scannen. Wenn sich also die DMZ-Server auf die Netzwerk-Firewall zum Internet hin verlassen, dann kann was schief gehen. Auch gegen Konfigurationsfehler und menschliches Versagen, das „nur“ die Netzwerk-Firewalls betrifft, hilft es in vielen Fällen.

Darum:

- Konfigurieren Sie auf jedem der Rechner in der DMZ, im Backend und bei den Clients die Queues „IN“ und „OUT“
- Versuchen Sie, möglichst mit Templates zu arbeiten, d.h. es gibt Regeln, die für alle (zumindest im gleichen Netz-Segment) gelten und solche, die Dienstspezifisch sind, also allein von der Aufgabe, die der jeweilige Rechner übernimmt, abhängen

Aufgabe 3.3: IP-Spoofing verhindern

Sofern Sie dies noch nicht gemacht haben, erweitern Sie alle Firewall-Regeln der Netzwerk-Firewalls so, dass

- Die Regeln das Interface miteinbeziehen (wenn Sie dies nicht machen, gelten die Regeln beim FORWARD auch spiegelverkehrt, d.h. z.B. gleichermaßen für Pakete von Innen wie von Außen – meistens nicht gewünscht)
- (Zusätzliche) Regeln das Senden von Paketen mit „falschen“ IP-Adressen verbieten:
    - Pakete mit richtigen IPs kommen über falsches Interface oder vom falschen Netzwerkbereich

Aufgabe 3.4: Firewall-Logs

Aus verschiedenen Gründen ist es erforderlich, dass die Firewalls mitloggen, was passiert. Dies dient zum Einen der Erkennung von Angriffen (alle abgelehnten Pakete), zum Anderen dem Debugging (warum geht meine Anwendung nicht). Wenn man keine andere Möglichkeit des Netzwerk-Monitorings hat, kann man durch das Mitloggen aller Verbindungen schon einen guten Eindruck gewinnen und diesen für andere Maßnahmen nutzbar machen.

Was brauchen Sie dazu?

- Konfiguration der LOG-Direktive auf den Netzwerk-Firewalls und den Host-Firewalls der DMZ-Server
- Anlegen eines lokalen Log-Servers auf den Netzwerk-Firewalls und den DMZ-Servern
  - Das Tool der Wahl ist üblicherweise SYSLOG, auch wenn dies auf UDP basiert und damit nicht garantiert, dass alle Pakete auch wirklich ankommen, wenn Log-Einträge von Rechner zu Rechner geforwarded werden
  - Sie können gerne auch andere Tools einsetzen, die Sie auf den Systemen installiert und konfiguriert bekommen
- Forwarden der Logs der äußeren Netzwerk-Firewall (zur Welt) sowie der Logs der Host-Firewall auf den DMZ-Servern auf die interne Netzwerk-Firewall
  - Hierfür sind natürlich Anpassungen der Firewall-Regeln notwendig!

Aufgabe 3.5: Überprüfung

Überprüfen Sie die Firewall-Regeln aktiv und nicht nur mit NETCAT:

- Testen Sie mit Hilfe von NMAP die Durchlässigkeit der Netzwerk-Firewalls sowie die Sichtbarkeit von Diensten für Angreifer
  - von der Welt scannen Sie die beiden Netzwerk-Firewalls, die DMZ und das Backend- sowie das Client-LAN (diese Vorgehensweise setzt beim Angreifer die Kenntnis Ihrer IP-Adressen voraus, aber zumindest bei der Verwendung öffentlicher IP-Adressen müssen Sie davon ausgehen, dass diese bekannt sind!)
  - von einem Server der DMZ scannen sie die anderen DMZ-Server und die beiden Netzwerk-Firewalls, das Backend- sowie das Client-LAN
- Überprüfen Sie die Scan-Ergebnisse und Logs der Firewalls anhand ihrer Erwartungen und korrigieren Sie ggf. die Konfigurationen der Firewalls
- Setzen Sie auf einem DMZ-Server TCPDUMP auf, und lassen Sie sich alle Pakete auf der Konsole ausgeben, die von der Welt durch die äußere Netzwerk-Firewall „durchkommen“. Führen Sie dann noch mal von der Welt einen NMAP-Scan auf die Server der DMZ aus und überprüfen Sie, ob wirklich nur die minimal notwendigen Pakete durchkommen.