Exploits und die SANS-Hitliste

Exploits sind Programme, die von Crackern ausgeführt werden und Schwachstellen in der Systemsicherheit ausnutzen. Außerdem werden wir einen Blick auf die Hitliste mit den zehn schwerwiegendsten Sicherheitslücken im Internet werfen, die die SANS-Gruppe aufgestellt hat.

Exploits

Wenn Sie herausfinden wollen, welche Tore geöffnet und welche geschlossen sind, dann ist die Reconnaissance von größter Wichtigkeit. Der nächste Schritt des Crackers besteht aber nun darin, tatsächlich in das Computernetzwerk einzudringen. Dies tut er, indem er Schwachstellen in Betriebssystemdiensten ausnutzt.

Den richtigen Exploit zu finden kann einem ganz schön Kopfschmerzen bereiten – es gibt so unglaublich viele davon. Exploits sind nicht alle gleich, sondern in der Regel von einem bestimmten Betriebssystem abhängig. Nur weil es einen Drucker-Exploit für Linux gibt, heißt das noch lange nicht, dass dieser unter Solaris läuft; umgekehrt gilt das gleiche.

Damit ich Ihnen besser erklären kann, was genau ein Exploit eigentlich ist und wie er , führe ich an dieser Stelle das Ausgabelisting eines Exploit sowie einige Pakete auf, die damit in Zusammenhang stehen. Zunächst möchte ich Ihnen jedoch einpaar Hintergrundinformationen zum von mir ausgewählten Exploit geben. Im Spätherbst des Jahres 2000 z.B. wurden zunehmend Aktivitäten zur Überwachung des Ports 515 beobachtet, die durch einen Exploit im Line Printer Daemon von Red Hat Linux 7.0 verursacht wurden. Auch jetzt – zum Zeitpunkt der Abfassung dieses Buches – fängt meine Firewall immer wieder Anfragen an diesen Dienst ab.

Hier sind die versprochenen Listings, versehen mit ein paar Anmerkungen

```
+++ Exploit information
+++ Victim: 192.168.1.25
+++ Type: 0 - RedHat 7.0 - Guinesss
+++ Eip address: 0xbffff3ec
+++ Shellcode address: 0xbffff7f2
+++ Position: 300
+++ Alignment: 2
+++ Offset 0

+++ Attacking 192.168.1.25 with our format string
+++ Brute force man, relax and enjoy the ride ;>
```

Aus der Zeichenkette `Type 0 - RedHat7.0 - Guinesss` können wir ersehen, dass der Exploit einen Zeilendrucker unter Red Hat 7.0 attackiert. Wollen Sie mal sehen, wie dieser Angriff für tcpdump aussieht?

```
18:34:19.991789 > 192.168.1.25.printer: S
4221747912:4221747912(0) win 32120 <mss 1460.sackOK.timestamp 4058996
0,nop,wscale 0> (DF) (ttl 64, id 11263)
              4500 003c 2bff 4000 4006 8b4e c0a8 0105
              c0a8 0119 0b4e 0203 fba2 c2c8 0000 0000
              a002 7d78 8bb1 0000 0204 05b4 0402 080a
              003d ef74 0000 0000 0103 0300
18:34:19.993434(0) ack 42217478913 win 32120 <mss 1460,sackOK,timestamp
393475 4058996,nop,wscale 0> (DF) (ttl 64, id 3278)
              4500 003c 0cce 4000 4006 aa7f c0a8 0119
              c0a8 0105 0203 0b4e 17b1 13ff fba2 c2c9
              a012 7d78 5ee7 0000 0204 05b4 0502 080°
              0006 0103 003d ef74 0103 0300
18:34:19.993514 >192.168.1.5.2894 >192 168.1.25.printer: . 1:1(0) ack 1 win
```

```
32120 <nop,nop,timestamp 4058996 393475> (DF) (ttl 64, id 11264)
```

Schauen wir doch mal, was hier passiert. Wir sehen zunächst, dass die Hosts `192.168.1.5` und `192.268.1.25` eine Verbindung herzustellen versuchen – ganz nach dem typischen Muster mit Threeway Handshake. In der nächsten Sequenz stellen wir dann fest, dass `192.168.1.5` versucht, den Exploit gegen `192.168.1.25` einzusetzen. Zum guten Ende verschiebt dann `192.168.1.5` 423 Datenbytes auf `192.268.1.25`. Der Exploit macht eine Weile so weiter, bis er schließlich in der Lage ist, eine Brute-Force-Attacke zu reiten.

Nach Abarbeitung des Exploits erhielt ich von `192.168.1.25` eine Shell (nicht, dass ich diese benötigt hätte) und konnte von nun an tun und lassen, was ich wollte.

Exploits sind die Eintrittskarte, mit der Cracker in ein System gelangen. Um sich gegen sie zu schützen, müssen Sie Ihre Betriebssysteme mit den entsprechenden Patches aktualisieren – das gilt für *alle* Systeme!

written by teTeX
m1r4b3ll15@gmail.com
http://tetex.dl.am

http://darkshadows.dl.am