Friedrich-Alexander-Universität
Erlangen-Nürnberg

Tobias Limmer
David Eckhoff
Christoph Sommer
Tilo Müller
Michael Gernoth
Reinhard Tartler

Netzwerk- und Systemsicherheit WS 2010/11

Cracking-Challenge 2.0, 25.01.2011

Netzwerksicherheit

In dieser Challenge sollen von uns betriebene unsichere Webshops gecrackt werden. Ziel ist es, in den insgesamt sechs von sieben Webshops zu einem Preis einzukaufen, welcher deutlich kleiner ist als der vorgesehene. Webshop 7 soll einen sicheren Webshop darstellen.

Das Gateway für die Webshops ist unter `bienenstock.informatik.uni-erlangen.de` zu finden. Unter diesem Hostnamen können alle Webshops erreicht werden. Grundlage für die Angriffe auf die Shops bildet die Methodik, die in Übung 09 vorgestellt wurde. Unter Umständen müssen auch verschiedene Angriffsarten kombiniert werden.

Bestellen Sie in mindestens 3 Webshops unter Ihrem Gruppennamen zu günstigeren Konditionen als vorgesehen. Bitte achten Sie darauf, dass Sie die gefälschte Bestellung mit Ihrem Gruppennamen abschicken. Legen Sie eine Beschreibung Ihrer Angriffe in der Textdatei `aufgabe09.txt` im Verzeichnis `aufgabe09` in unserem Abgabesystem ab. In dieser Aufgabe werden keien automatischen Tests bei Abgabe durchgeführt. Bei Problemen melden Sie sich beim Netsec-Team (`netsec@i7.informatik.uni-erlangen.de`). Die Bestellfrist endet am 07.02.2011.

Systemsicherheit

Zum Lösen dieser Aufgabe benötigen Sie lokalen Benutzer-Zugriff auf `bienenstock.informatik.uni-erlangen.de`. Lösen Sie dazu zunächst die Netzwerksicherheitsaufgabe oder, falls Sie nur Systemsicherheit hören oder an der Netzwerksicherheits-Aufgabe scheitern, verwenden Sie alternativ folgende Backdoor:

Vulnerability:	Bugtraq ID 45150
Affected:	ProFTPD 1.3.3c
Severity:	Critical
Published:	02 Dec 2010 by Daniel Austin

Anschließend sollen durch User Privilege Escalation Root-Rechte erlangt werden. Tipps:

Vulnerability:	CVE-2010-3847
Affected:	glibc 2.12.1 and others
Severity:	Critical
Published:	18 Oct 2010 by Tavis Ormandy

Vulnerability:	CVE-2010-3904
Affected:	Linux 2.6.30 to 2.6.38-rc8
Severity:	Critical
Published:	19 Oct 2010 by Dan Rosenberg

Geben Sie eine Beschreibung Ihres Vorgehens und funktionierende Exploits wie bisher über SVN ab. Zusätzlich können Sie im Home-Verzeichnis von Root eine kurze Textdatei anlegen, die den Erfolg Ihrer Gruppe bezeugt (bspw. *GruppeX was here*). In dieser Übung gibt es keine Punte wie bisher; zum Bestehen der Übung müssen Sie auf mindestens einem Weg Root werden. Abgabeschluss ist der 07.02.2011.

Hinweise

- Für Studenten die *nur* Netzwerksicherheit oder *nur* Systemsicherheit hören ist die Lösung der jeweils anderen Aufgabe freiwillig und kann, muss aber nicht, abgegeben werden.
- Da Sie im Verlauf dieser Aufgabe nicht nur lokale Benutzerrechte, sondern auch Root-Rechte erlangen, weisen wir Sie ausdrücklich darauf hin, dass jeglicher Missbrauch dieses privilegierten Zugriffs untersagt ist – *insbesondere die Behinderung anderer Übungsteilnehmer*. Nehmen Sie keine Änderungen am System vor sobald Sie Root geworden sind; Ihr Verhalten wird durch umfangreiches Monitoring geloggt.