Port-Knocking

Ingo Blechschmidt
<iblech@web.de>

LUGA

4. Mai 2005

Inhalt

Allgemeine Idee

Problem

Lauschen von Diensten $\Rightarrow$ Angriffspunkt

Lösung

Freischalten bestimmter Dienste erst nach einer „Anklopfsequenz“ $\Rightarrow$ Machtlose(re) Angreifer

Wichtig

Nicht Vernachlässigung der Sicherheit der durch Port-Knocking geschützten Dienste!

Allgemeine Idee

Problem

Lauschen von Diensten $\Rightarrow$ Angriffspunkt

Lösung

Freischalten bestimmter Dienste erst nach einer „Anklopfsequenz“ $\Rightarrow$ Machtlose(re) Angreifer

Wichtig

Nicht Vernachlässigung der Sicherheit der durch Port-Knocking geschützten Dienste!

Umsetzung

1. Schließen von Port p
2. Warten auf Anklopfsequenz
   (z.B. UDP-Pakete an vorbestimmte Ports)
3. Freischalten von Port p, evtl. Starten eines Dienstes, etc.

Mögliche Anklopfsequenzen

- UDP- oder TCP-Ports
- E-Mail
- Eintrag in einem öffentlichen Gästebuch,
  Einträge in öffentlichen Gästebüchern

Umsetzung

1. Schließen von Port p
2. Warten auf Anklopfsequenz
   (z.B. UDP-Pakete an vorbestimmte Ports)
3. Freischalten von Port p, evtl. Starten eines Dienstes, etc.

Mögliche Anklopfsequenzen

- UDP- oder TCP-Ports
- E-Mail
- Eintrag in einem öffentlichen Gästebuch,
  Einträge in öffentlichen Gästebüchern

Umsetzung

1. Schließen von Port p
2. Warten auf Anklopfsequenz
   (z.B. UDP-Pakete an vorbestimmte Ports)
3. Freischalten von Port p, evtl. Starten eines Dienstes, etc.

Mögliche Anklopfsequenzen

- UDP- oder TCP-Ports
- E-Mail
- Eintrag in einem öffentlichen Gästebuch,
  Einträge in öffentlichen Gästebüchern

Umsetzung

1. Schließen von Port p
2. Warten auf Anklopfsequenz
   (z.B. UDP-Pakete an vorbestimmte Ports)
3. Freischalten von Port p, evtl. Starten eines Dienstes, etc.

Mögliche Anklopfsequenzen

- UDP- oder TCP-Ports
- E-Mail
- Eintrag in einem öffentlichen Gästebuch,
  Einträge in öffentlichen Gästebüchern

Umsetzung

1. Schließen von Port p
2. Warten auf Anklopfsequenz
   (z.B. UDP-Pakete an vorbestimmte Ports)
3. Freischalten von Port p, evtl. Starten eines Dienstes, etc.

Mögliche Anklopfsequenzen

- UDP- oder TCP-Ports
- E-Mail
- Eintrag in einem öffentlichen Gästebuch,
  Einträge in öffentlichen Gästebüchern

Umsetzung

1. Schließen von Port p
2. Warten auf Anklopfsequenz
   (z.B. UDP-Pakete an vorbestimmte Ports)
3. Freischalten von Port p, evtl. Starten eines Dienstes, etc.

Mögliche Anklopfsequenzen

- UDP- oder TCP-Ports
- E-Mail
- Eintrag in einem öffentlichen Gästebuch,
  Einträge in öffentlichen Gästebüchern

Vor- und Nachteile

Vorteile

- Sichereres System durch Diensteabschottung
- Keine einfache Möglichkeit, auf die Anwendung von Port-Knocking zu testen

Nachteile

- Umständlicheres Verbinden
- Ausschließliche Verwendung einiger Ports für's Port-Knocking
- Fehler in Port-Knocking-Software $\Rightarrow$ Unerreichbarkeit

Vor- und Nachteile

Vorteile

- Sichereres System durch Diensteabschottung
- Keine einfache Möglichkeit, auf die Anwendung von Port-Knocking zu testen

Nachteile

- Umständlicheres Verbinden
- Ausschließliche Verwendung einiger Ports für's Port-Knocking
- Fehler in Port-Knocking-Software $\Rightarrow$ Unerreichbarkeit

Implementationen

„Perl prototype“ von portknocking.org

- Zahlreiche Features
- Nicht ganz einfache Konfiguration

„knock”

- Anklopfsequenz: Nur vorbestimmte UDP- oder TCP-Ports
- Sehr einfache Konfiguration

Implementationen

„Perl prototype“ von portknocking.org

- Zahlreiche Features
- Nicht ganz einfache Konfiguration

„knock”

- Anklopfsequenz: Nur vorbestimmte UDP- oder TCP-Ports
- Sehr einfache Konfiguration

knock

- ```
  # apt-get install knockd        # bzw.
  # emerge knock
  ```
- ```
  # $EDITOR /etc/knockd.conf
  [startSSH]
    sequence    = 42000,23000,1337
    seq_timeout = 5
    command     = /etc/init.d/sshd start
    tcpflags    = syn
  ```
- ```
  # /etc/init.d/knock start
  ```
- ```
  $ knock server 42000 23000 1337
  $ ssh iblech@server
  ...
  ```

knock

- ```
  # apt-get install knockd        # bzw.
  # emerge knock
  ```
- ```
  # $EDITOR /etc/knockd.conf
  [startSSH]
    sequence    = 42000,23000,1337
    seq_timeout = 5
    command     = /etc/init.d/sshd start
    tcpflags    = syn
  ```
- ```
  # /etc/init.d/knock start
  ```
- ```
  $ knock server 42000 23000 1337
  $ ssh iblech@server
  ...
  ```

knock

- ```
  # apt-get install knockd        # bzw.
  # emerge knock
  ```
- ```
  # $EDITOR /etc/knockd.conf
  [startSSH]
    sequence    = 42000,23000,1337
    seq_timeout = 5
    command     = /etc/init.d/sshd start
    tcpflags    = syn
  ```
- ```
  # /etc/init.d/knock start
  ```
- ```
  $ knock server 42000 23000 1337
  $ ssh iblech@server
  ...
  ```

Literatur

- `http://www.portknocking.org/view/resources/`
  Viele weitere Literaturverweise
- Linux-Magazin 12/2004
  „Port-Knocking: Die unsichtbare Hintertür“