Tracciamento dinamico dell'attività del kernel

Applicazioni alla sicurezza informatica

Emanuele Rocca

Dipartimento di Informatica e Scienze dell'Informazione

17 ottobre 2009

Generalità

SystemTap è uno strumento per Linux che consente di analizzare nel dettaglio il comportamento del kernel (dynamic tracing).

Generalità

SystemTap è uno strumento per Linux che consente di analizzare nel dettaglio il comportamento del kernel (dynamic tracing).

- Utilizzabile mediante un apposito linguaggio di scripting

Generalità

SystemTap è uno strumento per Linux che consente di analizzare nel dettaglio il comportamento del kernel (dynamic tracing).

- Utilizzabile mediante un apposito linguaggio di scripting
- Gli script vengono tradotti in C e quindi compilati per produrre un modulo del kernel

Generalità

SystemTap è uno strumento per Linux che consente di analizzare nel dettaglio il comportamento del kernel (dynamic tracing).

- Utilizzabile mediante un apposito linguaggio di scripting
- Gli script vengono tradotti in C e quindi compilati per produrre un modulo del kernel
- Paradigma di programmazione ad eventi

Generalità

SystemTap è uno strumento per Linux che consente di analizzare nel dettaglio il comportamento del kernel (dynamic tracing).

- Utilizzabile mediante un apposito linguaggio di scripting
- Gli script vengono tradotti in C e quindi compilati per produrre un modulo del kernel
- Paradigma di programmazione ad eventi
- Varie librerie di script (chiamate tapset) per analizzare le tipologie di eventi più interessanti

Generalità

SystemTap è uno strumento per Linux che consente di analizzare nel dettaglio il comportamento del kernel (dynamic tracing).

- Utilizzabile mediante un apposito linguaggio di scripting
- Gli script vengono tradotti in C e quindi compilati per produrre un modulo del kernel
- Paradigma di programmazione ad eventi
- Varie librerie di script (chiamate tapset) per analizzare le tipologie di eventi più interessanti
- Non richiede specifiche conoscenze a livello kernel

Generalità

SystemTap è uno strumento per Linux che consente di analizzare nel dettaglio il comportamento del kernel (dynamic tracing).

- Utilizzabile mediante un apposito linguaggio di scripting
- Gli script vengono tradotti in C e quindi compilati per produrre un modulo del kernel
- Paradigma di programmazione ad eventi
- Varie librerie di script (chiamate tapset) per analizzare le tipologie di eventi più interessanti
- Non richiede specifiche conoscenze a livello kernel
- Affidabile, niente disastri in ambienti di produzione

Generalità

SystemTap è uno strumento per Linux che consente di analizzare nel dettaglio il comportamento del kernel (dynamic tracing).

- Utilizzabile mediante un apposito linguaggio di scripting
- Gli script vengono tradotti in C e quindi compilati per produrre un modulo del kernel
- Paradigma di programmazione ad eventi
- Varie librerie di script (chiamate tapset) per analizzare le tipologie di eventi più interessanti
- Non richiede specifiche conoscenze a livello kernel
- Affidabile, niente disastri in ambienti di produzione
- Software libero, sviluppato tra gli altri da Intel, IBM, Hitachi, Red Hat, Oracle

Esempio di script: scansioni FIN, NULL e XMAS

```
probe tcp.receive {
    name = ""

    if (fin && psh && urg) name = "XMAS";

    if (!psh && !urg && !syn && !rst && !ack)
        name = fin ? "FIN" : "NULL";

    if (name != "") printf("\n%s scan detected", name);
}
```

Intrusion Detection System

- Strumenti per rilevare potenziali tentativi di intrusione
- Possono essere di rete o host based
- Possono essere basati sull'analisi delle anomalie
- Tra i vari approcci: analisi delle sequenze di chiamate di sistema, Forrest et al.
- Durante l'analisi si confronta il comportamento del sistema con la definizione di normalità
- Si segnalano i comportamenti anomali
- Necessitano di una fase iniziale di addestramento

Implementazione di un IDS mediante SystemTap: sequenze di chiamate di sistema

Il sistema sviluppato utilizza un database di sequenze di syscall eseguite dai vari programmi come definizione di normalità.
La parte centrale del sistema è uno script SystemTap che genera la lista delle sequenze eseguite. Per esempio:

```
pulseaudio 1000 gettimeofday sendto send gettimeofday
pulseaudio 1000 sendto send gettimeofday poll
rhythmbox 1000 poll gettimeofday recvmsg gettimeofday
rhythmbox 1000 gettimeofday recvmsg gettimeofday poll
rhythmbox 1000 recvmsg gettimeofday poll gettimeofday
```

Creazione del database

```
staprun allsequences.ko | python builddb.py
Loading old data... done
Updating database. Stop at any time with CTRL+C
^CDone
Creating backup file /var/tmp/ids.db.old... done.
Database built into /var/tmp/ids.db
Unique syscalls sequences per executable name:
gnome-screensaver 771
less 204
gnome-pty-helper 79
[...]
```

Riconoscimento delle intrusioni: rootkit ark

```
staprun allsequences.ko | python runtime_check.py
6 netstat ('rt_sigprocmask', 'fork', 'rt_sigaction',
           'rt_sigaction', 'rt_sigprocmask', 'wait4')
6 netstat ('fork', 'rt_sigaction', 'rt_sigaction',
           'rt_sigprocmask', 'wait4', 'rt_sigaction')
6 netstat ('rt_sigaction', 'rt_sigaction', 'rt_sigprocmask',
           'wait4', 'rt_sigaction', 'rt_sigaction')
6 netstat ('rt_sigaction', 'rt_sigprocmask', 'wait4',
           'rt_sigaction', 'rt_sigaction', 'rt_sigprocmask')
```

Riferimenti

http://www.linux.it/~ema/tesi.pdf

http://bitbucket.org/ema/systemtap-ids-poc/overview/