Řešení pro audit činnosti administrátorů UNIX/Linux serverů

OpenSource řešení v sítích
29. 10. 2009, Karviná

Pavel Běhal

Agenda

- Úvod do problému
- Dostupné prostředky
- Technické řešení
- Kousek zdrojového kódu
- Problémy & Rizika
- Jiná řešení

Úvod do problému

- Rozsáhlé, mezinárodní IT prostředí
- Relativně homogenní UNIX/Linux svět
- Provoz tzv. „interního outsourcingu“
  - nejen na úrovni aplikací, ale pouhých platforem (server s OS)
- Nutná široká sdílená znalost hesla systémových a aplikačních účtů
- Problémy s popiratelností odpovědnosti ze strany interních i „třetích“ administrátorů

Dostupné prostředky

- Politika zákazu používat systémové / aplikační účty přímo *(root, oracle, ...)*
- Vynucované:
  - *„su“*
  - *„sudo“*
  - *používání komplexních „zástupných“ skriptů*
- Pokusy se shellem:
  - *„script“*

Technické řešení (1/3)

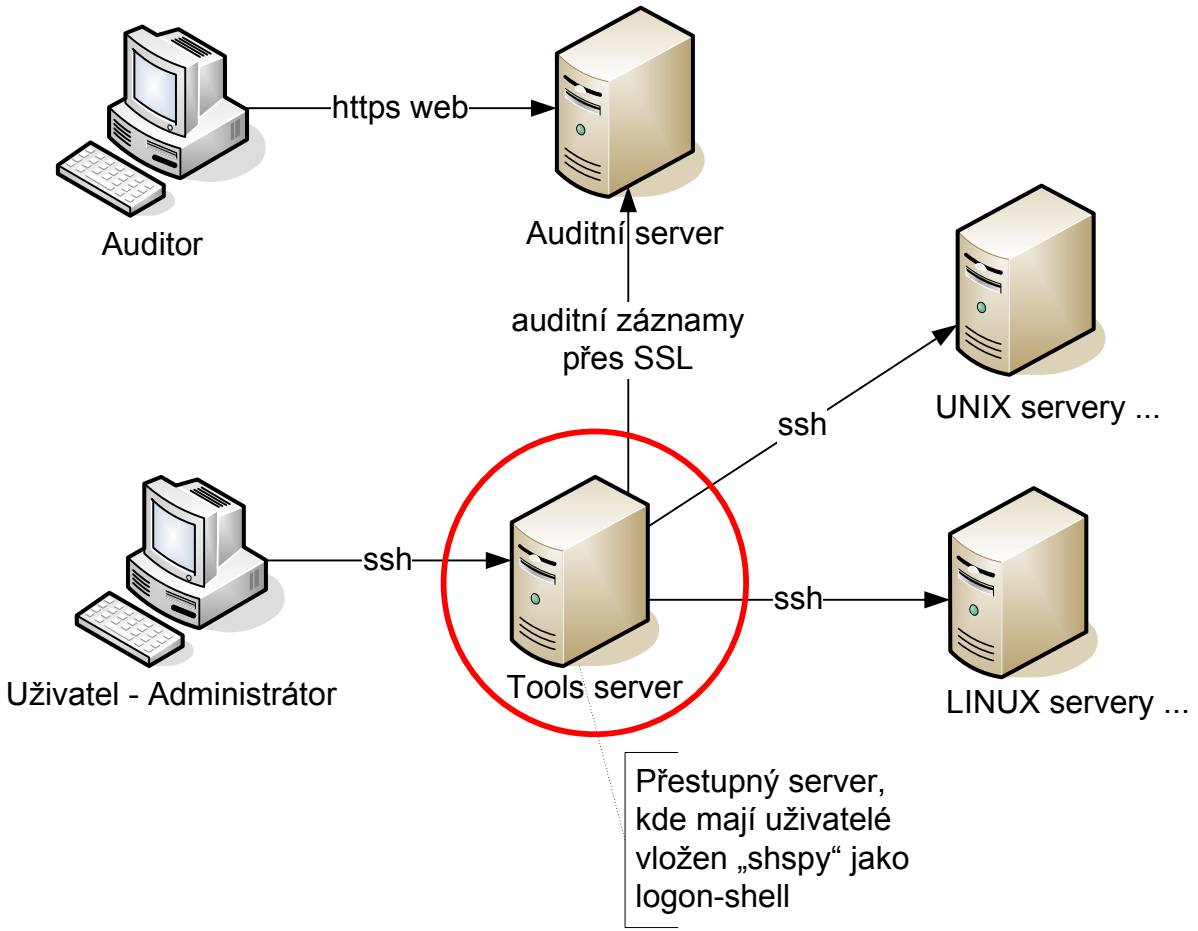
- Zadání:
  - efektivní zaznamenávání práce administrátorů
  - přenositelnost mezi různými UNIX/Linux verzemi
  - minimální dopad na samotné servery
  - centralizované řešení
  - šifrování a řízení přístupu
  - rozhraní pro autorizované administrátory a auditory *(vyhledávání, přehrávání)*

- Zákaznický vývoj z důvodu úspory nákladů za licence

Technické řešení (2/3)

- Výsledek:
  - Shell wrapper „shspy“
    - Náhrada „login shellu“ sledovaných uživatelů
    - Zachytává STDIN a STDOUT z terminálové session
      - *stisknuté klávesy, vytištěný text, přenesená data*
    - Podporované funkce:
      - interaktivní přihlášení (login, ssh, telnet, rlogin)
      - spouštění lokální příkazů (su)
      - spouštění vzdálených příkazů (ssh, rsh – včetně zachytávání „roury“)
      - zachování funkcí SSH sftp a scp
    - Dočasné ukládání záznamů na lokálním disku
  - Agent pro přenos dat na centrální auditní server
  - Centrální auditní server:
    - Bezpečné úložiště záznamů se řízením přístupů
    - Grep a fulltext vyhledávání, přehrávač session a jejich částí

Technické řešení (3/3)



Kousek zdrojového kódu (1/2)

```
... inicializuje se virtuální terminál PTY
for(;;) {
   ...
   n = select(nfd, &readmask, (fd_set *) 0, (fd_set *) 0, (struct
   timeval *) 0);
   if(n < 0) {
        if(errno == EINTR) continue;
        terror("select",LOG_ERR,1,1);
        return(1);
   }
   /* input from slave fdprocess */
   if(FD_ISSET(fdprocess, &readmask)) {
        if((n = read(fdprocess, buf, sizeof(buf))) <= 0) {
                /* slave process died */
                DEBUG_L2_PRINTF("midle_loop(): slave process died -->
   exiting\n", n);
                return(0);
        }

        if(log_write_out) log_write_out(buf, n);
        write(STDOUT_FILENO, buf, n);
   }
```

Kousek zdrojového kódu (2/2)

```
    /* input from user */
    if(FD_ISSET(STDIN_FILENO, &readmask)) {
          if((n = read(STDIN_FILENO, buf, sizeof(buf))) < 0) {
                    // Not a terminal, maybe background process
                    continue;
                    /* terror("read stdin");
                    exit(1); */
          }
          /* end of input */
          if(n == 0) {
                    DEBUG_L2_PRINTF("midle_loop(): user process closed stdin -->
    exiting\n", n);
                    return(0);
          }
          if(log_write_in) log_write_in(buf, n);
          if(write(fdprocess, buf, n) != n) {
                    terror("write pty",LOG_ERR,1,1);
                    return(1);
          }
    }
    /* rotate logs */
    if (bytes_written_in + bytes_written_out >= BYTES_LIMIT) {
          ... rotace výstupních záznamů
    }
}
```

Problémy & Rizika

- Problémy:
  - Zásah do „tty“ vrstvy a její logiky
  - Asynchronnost terminálového přenosu
  - Stabilita vůči signálům
  - „NOECHO“ režim terminálů
  - Detekce ukončení / upadnutím / timeoutu session
  - Detekce použití v režimech: *příkaz bez terminálu, „roura“ a přenos souborů*

- Rizika:
  - Změna „login shellu“ uživatelem
  - Riziko „úniku ze shellu“ *(„X“ aplikace, vzdálené příkazy SSH, ...)*
  - Zachytávání i aplikačních hesel
  - Lokální i centrální zabezpečení zaznamenaných informací
  - Útok promazáním lokální diskové cache
  - Volné místo na disku sledovaného serveru
  - Zahlcení centrálního auditního serveru *(objem dat)*

Jiná řešení

- Enterprise Audit Shell (eas, v. 2.0 z 28.3.2006)
  - již nevyvíjeny, ale stále dostupný OpenSource produkt, autor se vrhnul na komerční verzi
  - http://search.rpmseek.com, klíčové slovo „eas“
- *Shell Control Box fy. Balabit*
  - *komerční řešení od autora syslog-ng*
  - *http://www.balabit.com*
- *Direct Audit fy. Centrify*
  - *komerční řešení vázané na MS Active Directory*
  - *http://www.centrify.com*

Děkuji Vám za pozornost

Otázky & Odpovědi