痕跡に注目したログ収集機能の検討

4T－7

－ リモートアタックへの拡張 －

女部田　武史[1)]，岡澤　俊士[2)]，浅香　緑[1)]
情報処理振興事業協会技術センター[1)]，（株）日本総合研究所セキュリティ事業推進部[2)]

1　はじめに

コンピュータへの不正侵入の増大に伴って侵入検出のための技術が強く要求されてきている。こうした背景の中、情報処理振興事業協会では独自の侵入検出手法を用いた侵入検出システムの開発を行っている。我々の提案する手法は侵入事例で観察される侵入行為の結果（痕跡）を初期情報として侵入検出を行うものである[1]。具体的には侵入を検出する場合にはじめに侵入行為の結果残される事象（痕跡）を検出し、次に痕跡情報に従って関連する詳細なログを収集し、侵入を判定する。この手法によって、収集するログの量の大幅削減、判定の効率や精度の改善、未知の侵入手口への対応などを期待することができる。

これまで本方法が不正侵入の中のローカルアタックと呼ばれる手法に対して効果があることを検証してきた[2]。今回はリモートアタックに本方法を拡張することを試みたので報告する。

2　侵入行為への適用

侵入行為を以下の 2 つに分けて、痕跡を用いた侵入検出方法の適用を検討した。

- **ローカルアタック**
  侵入者がすでにマシン上にアカウントを持ち、有している以上の権限を奪おうとする攻撃。
- **リモートアタック**
  侵入者が直接的にマシンにアカウントを持たない場合に行う攻撃。

ローカルアタックに対しては 1)ルートシェルの起動、2)重要なファイルの修正の 2 つを痕跡として侵入判定を行うことで、158 件のローカルアタックのうち 95％を検出することが可能であるという結果が得られた[2]。

2.1 リモートアタックへの拡張

痕跡を用いた侵入判定方法をリモートアタック検出に拡張するにあたっては以下の 3 つの問題がある。

1. 収集するログの種類（どのログを収集するか）
2. ログ収集方法（どのようにログを収集するか）
3. 痕跡の定義（何を痕跡とするか）

上記の問題を解決するために、実際にリモートアタックの攻撃ツールでシステムを攻撃し、どのようなログが残るのか調査してリモートアタックにおける痕跡の定義を行った。

2.2 リモートアタックの分類

研究に先立ってリモートアタックの調査を行った。以下にリモートアタックの手口の分類について示す。これは過去 4 年間インターネット上で公開されていたツールである。合計で 41 のツールを収集した。

① **バッファオーバーフロー　(7 / 41)**
statd や mountd などのデーモンプロセスのバッファをオーバーフローさせてデーモンの権限で任意のコマンドやシェルを実行するもの。

② **重要ファイルの修正、作成 (13 / 41)**
CGI や sendmail などのバグをついて passwd ファイルなどを参照、修正したりするもの。

③ **パケットの偽造 (2 / 41)**
不正なパケットを生成して、telnet などのセッションを奪うもの。

A Study of How to Find Marks of Intrusion from System Logs. – Applying to remote attack-
Takefumi Onabuta[1)], Shunji Okazawa[2)], Midori Asaka[1)]
Information Technology Promotion Agency[1)], The Japan Research Institute, Limited[2)]
Bunkyo Green Court Center Office. 2-28-8. Honkomagome. Bunkyo-ku. Tokyo 113-6591. Japan

④ **パケットの盗聴 (5/ 41)**
ネットワーク上を流れるパケットを盗聴してパスワードなどを盗むもの。

⑤ **スキャンニング (5 / 41)**
提供されているサービスの情報やマシンの情報を検索するもの。

⑥ **その他 (9 / 41)**
トロイの木馬やパスワードクラックなど。

リモートアタックはローカルアタックに比べてその攻撃方法が多岐にわたっている。

2.3 収集するログの種類

ローカルアタックを判定するためには以下の 8 種類のシステムコールを監視した。

execv, fork, open(write), creat,
chmod, chown, chmod symlink

リモートアタック検出のためにはこの他に *open(read)*とネットワーク関連のログとして、以下のシステムコールを監視した。

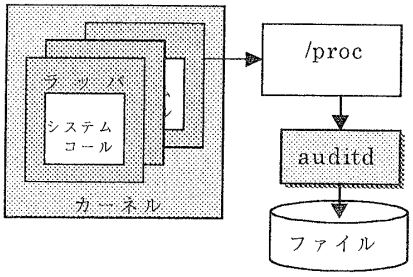
getmsg, socket connect,
socket send, putmsg

*open(read)*を監視する理由はリモートアタックではパスワードファイルなど重要なファイルを無許可で参照するものが多いためである。またリモートアタックではソケットを通じて不正な情報のやり取りが行われるケースが多いためネットワーク関連のシステムコールも監視する。

2.4 ログ収集の方法

ローカルアタックにおいてはログ収集のために Sun の BSM (Basic Security Module) を利用した。しかし BSM では login による認証を受けていないプロセスのログを出力しないので、リモートアタックのログを収集することができない。そこで今回は Linux 上 (RedHat5.2) に BSM と同様な機能を持つ audit システムを構築した。

audit システムでは Linux のシステムコール 152 個の内ファイルシステム関係、およびプロセス関係のシステムコールにログ出力用のラッパーコードを仕掛けて、/proc 上にログを書き出すようにした。/proc に書き出したログをデーモンプログラムでフィルタリングしながら特定のファイル上に記録する。



上記のツールを利用して、2.2 で調査したリモートアタックを実行し、ログを収集した。実験ではバッファオーバーフローと重要ファイルの修正に分類されたツールのみを調査した。ログは以下のような形式で出力される。

```
header, 240, 1, open, Tue Sept 1 16:11:44 1992
path, /etc/passwd
subject, root, nobody, nogroup, nobody, nogroup, 28
```

これらのログを解析し、リモートアタック上で痕跡となる事象（ログ）について検討した結果、以下の 2 つを痕跡として定義することで、リモートアタックの初期動作を検出できることがわかった。

- デーモンプロセスによるルートシェルの起動
- デーモンプロセスによる重要なファイルの修正、参照、作成 (/etc/passwd, /etc/shadow, /etc/hosts.equive, /.rhosts)

ローカルアタックでは setuid コマンドが攻撃の対象となるが、リモートアタックではデーモンプロセスが攻撃の対象となる。それぞれ攻撃対象は異なるものの、攻撃の結果行われる行為には共通性がある。

3 おわりに

痕跡を用いた侵入判定手法をリモートアタックに適用した結果を示した。リモートアタックの痕跡として 2 つのイベントがあることがわかった。今後はこれらを用いた侵入の判定方法を検討していく。

参考文献

[1] Midori.Asaka et al:"Local Attack Detection and Intrusion Route Tracing", IEICE Trans., to appear (1999)

[2] 田口,女部田,浅香:"痕跡に注目したログ収集機能の検討",情処学会第 56 回全国大会(1998)