実践セキュリティ特論 上原先生 第一回課題

28G23027
川原尚己

問１：脅威分析につかう STRIDE とは何か．各頭文字が持つ意味を簡単に説明せよ．

- Spoofing：なりすまし
- Tampering：改ざん
- Repudiation：否認
- Information Disclosure：情報漏洩
- Denial of Service：サービス拒否
- Elevation of Priviledge：特許の昇格

問２：C や C++で書かれたプログラムのバッファオーバーフロー対策として OS やライブラリで行われている工夫について調べ，説明せよ．

「StackGuard」というツールでは，リターンアドレスが書かれている前に「カナリア」という値を挿入している．バッファオーバーフローが発生してリターンアドレスが書き換わると，（素直な方法では）カナリアの値が変更され，実際に使用される前にシステムがバッファオーバーフローを検知することができる．

あるいは，Linux のカーネルを修正し，スタック・セグメント上でのプログラムの実行を禁止する方法もある．

問３：マルウェア対策として長く利用されてきたいわゆるウィルス対策ソフトウェアは最近その効果が疑問視されるようになってきた．その理由を述べ，代替の対策として考えられていることについて説明せよ．

ウイルス対策ソフトはすでに検出検出されたウイルスに含まれるパターンを検出することによって検出を行っている．そのため，標的型攻撃と呼ばれるある攻撃対象専用にカスタマイズされたマルウェアに対しては検出を行うことが困難である．代わりに，EDR と呼ばれる方法が考えられている．EDR では，パソコンやサーバーの状況や通信内容などを監視し，以上や不審な挙動があれば管理者に通知する．管理者は通知を受けた後，EDR で取得されたパソコンや通信の状況を示したログを分析して対策を講じる．