セキュリティ・スタジアム2004盛況のうちに終了

セキュリティ・スタジアム実行運営委員会
根津　研介

2004年11月2日～4日まで、大田区産業プラザ（PIO）特別会議室でセキュリティ・スタジアム2004を粛々と開催いたしました。エントリされた参加者も多い日には30余名になりましたが、ちょうど、期間中に国民の祝日（文化の日）を挟んだために、参加者もセキュリティ技術を研鑽するのに、所属団体／企業の業務の一環として参加される方や、個人のスキル向上として参加される方など開催日によって傾向が見えて、セキュリティ技術者をとりまく社会的な環境の「いま」を表しているのではないかと思われました。

ここで、セキュリティ・スタジアムの内容について簡単にご説明したいと思います。

セキュリティ・スタジアムは、参加者が「攻撃」、「防御」、「監視／検知」のいずれか（複数エントリも可能）として参加します。「攻撃」に参加する人は、防御として参加した方が立てているサーバを攻撃し、どのような形で攻撃が成立するのかを実地を通して学び、公開されているツールや脆弱性そのものの有効性を検証します。「防御」で参加する人は、たとえば防御として設定すべき内容がどこまでなのかや、普段自分が設定している防御方法の有効性の検証、それから、攻撃を受けたときに十分にログがとれているのかや、どのようなログがでてくるのかを実地で検証し、確認します。

「監視／検知」で参加する人は、このような攻撃と防御のトラフィックの中から、有効な攻撃がどのように行われたのかをいかに効率よく摘出できるか等の監視ルールの有効性の確認や、監視ツールの有効な範囲、自動アラート機能がどのようなパケットパターンを誤検知するかの検証などを行います。また、攻撃パターンのパケットを大量に収集できるというメリットもあります。

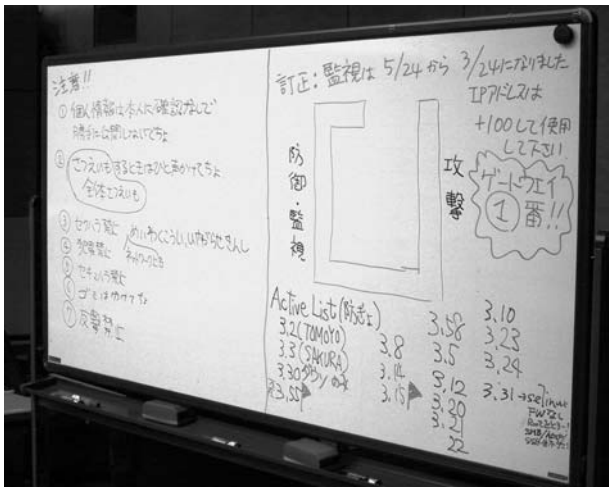
今回は、傾向として「攻撃」側として参加される参加者が多く、また、特徴としてセキュアOSワーキンググループからLinuxベースのセキュアOSであるTOMOYO Linuxと物理的に改ざんできない改造がなされているSAKURA Linuxが「防御」としてエントリしていただきました。この場を借りてお礼申し上げます。また、今回は特に「監査／検知」のエントリがほとんどありませんでしたが、今後、製品ラインアップをお持ちの企業の方の実証実験の場としても、ぜひ活用していっていただければと思います。

このような状況でしたので、若干防御側のマシンが不足したため主催者側が比較的防御レベルの低い防御マシンを数台用意して持ち込んでいました。この中には、実際に想定されるサーバの平均的な防御手段が講じられているものであったり、想定されうる限り弱いサーバなどがありました。つまり、インストールされただけのサーバもあり、また、SELinuxがオンになってはいるものの一切のパッケージアップデートが行われていないFedora Core 2などを防御側に持ち込んでいました。

また、先ほどとりあげたTOMOYO Linuxは、完全に設定されたものではまず攻略できないため、攻撃側の突くことのできる弱い部分を敢えて作り込んでおいていただき攻略のシナリオをいくつか用意していただきました。

三日間のセキュリティ・スタジアム競技を通して、いくつかの成果を得ることができました。主に、攻撃側の成果になりますが、まず、結果として、主催者側が用意した防御マシンはほぼ初日のうちに攻略されてしまいました。

また、TOMOYO Linuxは今回、参加者の注目の的であったため、多くの攻撃側参加者のターゲットになっていましたが、二日目になって、用意されていた脆弱性の



一つを通して攻略されました。今回、持ち込んでいただいたTOMOYO Linuxはファイルの実行権限やアクセス権が制限されており、apacheの構成ファイルやホームページは全て書き込み権限がないエリアに存在していたのですが、tomcatがインストールされていました。また、Sambaのバージョンが古くバッファオーバーフローの脆弱性が内在していました。これらに目をつけた参加者がSambaの脆弱性を利用してJavaプログラムをサーバー上にまんまと仕込み、apacheサーバを停止させることに成功すると、送り込んだJavaプログラムをtomcat経由で動作させてWebサービスを提供するようにしてしまったのです。これはネットワーク上からみると、まさしくホームページを書き換えたのと同じ結果を得ることができたことになります。

なお、主催者側が持ち込んだ防御側サーバの一つであるSELinuxがONのFedora Core 2ですが、宣伝不足のせいで三日間を通して攻略されることはありませんでした。「セキュアOS採用」という宣伝をすることによって、かえって攻撃者の心理に「なんとか落としてやろう」とする人間心理が垣間見えるような結果であったと言えるでしょう。

このように粛々と盛況な中でいくつかの成果も得ることができ、成功裏のうちにセキュリティ・スタジアム2004は無事、終了しました。今後、2005年の上半期中には今回の成果をふまえた上で、「セキュリティ・スタジアム2005」として、また、皆さんにご紹介できればと考えております。その際にはぜひ、より多くの方の参加とご協力のほどをお願いいたします。