Blackhat2001 DEFCON9

作成： HINET （（株）日立情報ネットワーク） moto@hinet.co.jp

日付：2001/07/26 http://www.shield.ne.jp/

1. ハッカーとクラッカー

動いている時計の仕組みを知りたくて時計を開けて調べる様な探求心旺盛なコンピュータのエキスパートがハッカーと呼ばれる。ハッカーが犯罪的行為に走るとクラッカーへと変貌する。但し、ハッカー達は世間が簡単に白黒つけている風潮には反感をもっており、スパイダーという呼び名をつくったり、悪い奴は Blackhat, 良い奴は Whitehat と呼ぼうとアナウンスしている。

USA TODAY(1999)

2. BLACKHAT2001

2001 年 7 月 10～12 日 アメリカ、ラスベガス

今年で 2 回目を数える、ハッカーが主催する米国政府のセキュリティ会社等の参加する公式なセキュリティカンファレンス。http://www.blackhat.com/

プログラムは全部で４０のスピーチで成り立っている。スピーカーもウイルスやウォーム、アタック・ツール、脆弱性データベース、ハニーポットやＩＤＳなどのネットワーク防御手法などセキュリティ全般にわたって選ばれていた。 今年特に注目となったのが、ワイアレスＬＡＮの脆弱さを露呈するスピーチだった。@ステイクのティム・ニューシャムは、ワイアレスＬＡＮの使うセキュリティであるＷＥＰ(Wired Equivalent Privacy) プロトコルに、パスワード・クラッキングの方法を当てはめて、その脆弱性を露呈している。また、最近の動向としては、人件費がかかるセキュリティ・コンサルティングをオートマ化する方法が模索されている。それを代表するスピーチが、CORE-SDI の人々によって行われた”ペネトレーション・テスト のオートマ化”である。その他、Nessus の紹介では、７月に投入されるバージョン1.2 の紹介（GUI が入ったこと、nmap のスキャンの結果を流用できること、パラレルスキャンなどによりテストの速度が増加したこと、CGI スクリプトをテストするプラグインの紹介などが行われている。Sourcefire Inc の Martin Roesch が行った Snort のスピーチでは、snort の紹介と、アップデートの情報が配布されている。紹介ではその使い方（スニッファー・モード、パケット・ロガー・モード、ネットワークＩＤＳモード、事件後検証モード）や snort のアーキテクチャーなどが紹介された。日本から唯一参加していたのはセキュリティフライデーの左内氏で、ARP パケットを使ったプロミスキャウス・ノードの検出について発表した。

BLAKHAT のオルガナイザ
ダーク・タンジェント

セキュリティフライディの
左内氏

2. DEFCON9

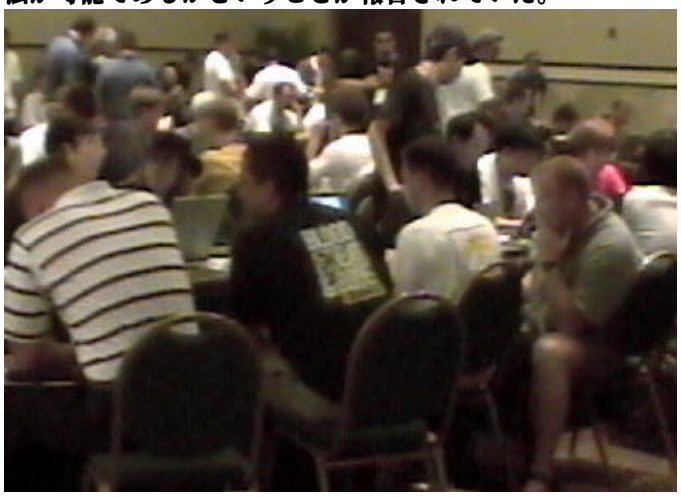
2001 年 7 月 10～12 日　アメリカ、ラスベガス

今年で９回目の DEFCON は年に 1 度のハッカー達の祭典である。コンファレンスの側面と、いわゆる“オフ会”の側面がある。
http://www.defcon.org/

Newbie、General、Uber Haxor(Super Hacker)の 3 つの Session と、Capture The Flag や Haxor Jeopardy（クイズ大会）などのさまざまな Event が行われる。

Haxor Jeopardy（クイズ大会）

Security & Privacy- An Introduction To Some Interesting Concepts では、Virus や Worm、DoS（Denial of Servis）、DDoS（Distributed DoS）、Sniffing、Spoofing のについてどんなものか、またそれらの手法について例を挙げながら説明していた。このセッションには 12 歳くらいの子供も参加していた。　TCP/IP Intelligent Agents: The Future of Electronic Warfare& Defense では将来の検知、対策ツールに関してのスピーチがあり、そこでは detect から response までを自動化するといったことが語られていた。FX"Attacking Control, Routing & Tunneling Protocals"（アタッキングコントロール、ルーティング、トンネリングプロトコル）最近の傾向としてアプリケーションレベルでの攻撃や、バグなどのセキュリティホールをついた攻撃が目立っており、ネットワークレイヤーに対する興味はあまりなかったのが現状であるが、レイヤー２と３にフォーカスしそれらがどういったもので、どういった攻撃方法が可能であるかということが報告されていた。



Capture The Flag の状況

Capture The Flag（CTF）これは、参加者たちで何名かのチームを作り、チーム内で攻撃ホスト、ターゲットホストを設置し、他のチームからの攻撃を凌ぎつつ、相手チームのシステムに侵入し、root 権限を奪取する（旗を奪う）というゲームである。Root 権限を奪取するとポイントが加算され、一番ポイントの多いチームが勝ちとなる。今回我々からも急遽参加することになり、おのおの持ちこんだノート PC をセットアップしてゲームを楽しんでいた。

以上