The A-Team
CS 480

From left to right
Alan Blair, Todd Denny, Paul DeVries, Eric Cray
Ian Dixon (not pictured)

System Configuration

- Windows XP - .195
  - Telnet
  - SSH
  - FTP
  - HTTP
  - Messenger
  - VNC
  - RPC
  - MySQL
  - PHP
  - simpleFileServer

User	Hidden	Admin
Team1	no	Yes
Guest	no	No
a-team	yes	No
t1	yes	No
t2	yes	No
t3	yes	No
user1	yes	No
user2	yes	No
user3	yes	yes

System Configuration Cont

- CentOS - .151
  - Services running
    - simpleFileServer
    - VNC
    - SSH
    - apache (latest stable release)
    - ftp
    - MySQL
    - NFS (as root)
    - Telnet
  - Accounts

team1 (admin)
t3
t1 (admin)

Defense Machines

Machines were installed with latest releases of most services.

- Win: apache, ftp, remote desktop, vpn

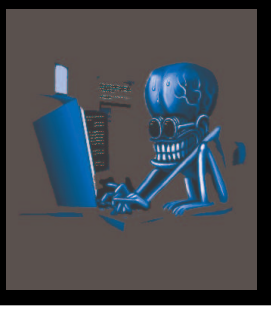
- Linux: apache, ssh, MySQL, dns, ftp

Modifications to Defense

- Windows XP SP 2
  - Deleted hidden accounts
  - Assigned a password to *defender* admin account
  - Installed ZoneAlarm firewall with low security
- Ubuntu
  - Reset *root* and *attackme* passwords

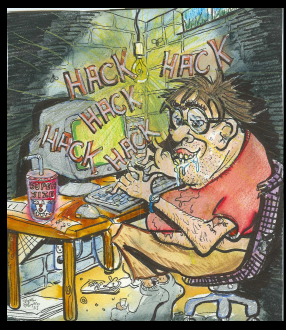
Detected Attacks

- No security breaches on either machines detected
- Users were trying to access Apache, but it was configured correctly and was the latest version



Offensive Measures

- Script Kiddie style
  - Used LinuxBacktrack for recon and attacks
    - Recon: Nessus, NMAP, SNScan, and LANGuard
    - Attack: Metasploit and Ninja (autopwn)
  - No successful meaningful attacks as systems were patched and firewalled too quickly



Offense .200

- Intelligent attacks
  - mail server

```
bt ~ # telnet 172.18.1.200 25
Trying 172.18.1.200...
Connected to 172.18.1.200.
Escape character is '^]'.
220 mail.domain.com ESMTP Merak 8.9.1; Wed, 18 Apr 2007 20:08:09 -0700
HALLO
500 5.5.1 Command unrecognized: "HALLO"
HELLO
500 5.5.1 Command unrecognized: "HELLO"
HELO
501 5.5.1 HELO/EHLO requires domain address
HELO www.google.com
250 mail.domain.com Hello www.google.com [172.18.1.149], pleased to meet you.
```

  - Remote Desktop
    - Allowed login, but could not actually do anything – only showed a black screen

Offense .155

- ftp server with anon login

```
bt ~ # ftp 172.18.1.155
Connected to 172.18.1.155.
220 emu_nt Microsoft FTP Service (Version 3.0).
Name (172.18.1.155:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
ftp>
```

- Spamming with messenger

```
C:\Documents and Settings\user3>net send 172.18.1.155 !!WARNING!! VIZIRUSES ARE
UP IN YOUR COMPUTZORZ!!
The message was successfully sent to 172.18.1.155.
```

Offense .148

- Apache 1.3.x installed initially
  - No attack attempted until second day, at which time it was patched to latest version
- Useful information gathered that could be used in future, but no known exploits existed

Offense .146

- Useful information gathered that could be used in future, but no known exploits existed

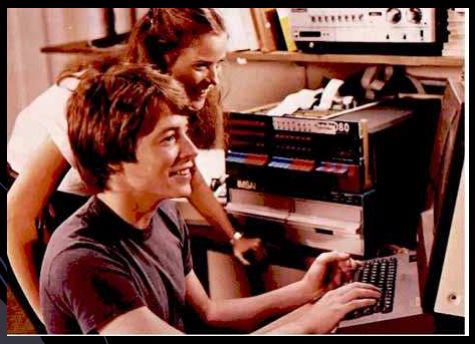
Eric (left) and Ian

Lessons Learned

- Learned very much about each machine and its processes
  - While no real exploits were available at the time, enough information was gathered so future exploits may be possible
- Putting up a firewall makes attacking very difficult
- Attacking would be more successful if there was traffic being generated from the machines
  - e.g. someone checking their e-mail or telnetting to a machine
  - Attacking is just as much about the machines as it is the traffic between them
  - Ethereal, Cain and Abel would have been useful tools
- Social engineering would probably have been successful in a real environment
  - Messenger service prone to spamming users with tasks
- Windows readily gives up information about available accounts, password rules, network shares and just about anything else you can think of

Lessons learned cont.

- It is possible to be a hacker without listening to stylish techno
- Being a Script Kiddie (1337 h4x0r) is easy. Many tools make it a no brainer (given systems that haven't been hardened)
- At no point did a girl ever enter the room and take interest in what we were doing.



Picture that gives false hope

Questions?

The quintessential hacker