



# Securitatea retelelor de calculatoare

**Sabin-Corneliu Buraga**

busaco@infoiasi.ro

<http://www.infoiasi.ro/~busaco/>





# Cuprins

- Preambul
- Vulnerabilitati
- Atacuri
- Prevenirea
- Supravietuirea





# Preambul

- **Securitatea**  $\equiv$  abilitatea de a evita neplacerile produse de **orice** risc, amenintare sau pericol
  - In practica, **imposibil** de realizat... ☹
- **Incident de securitate**  $\equiv$  eveniment aparut in cadrul retelei, cu implicatii asupra securitatii unui calculator sau a retelei
  - Provenind din **interiorul** ori **exteriorul** retelei





# Preambul

- Ce anume trebuie securizat:
  - Datele
  - Serviciile de retea (aplicatiile sau partile acestora)
- **Securitate fizica vs. securitate logica**
- **Cracker vs. hacker**





# Preambul

- Aspecte ale securitatii
  - **Confidentialitatea**
  - **Integritatea**
  - **Autenticitatea**
  - **Nerepudierea**
  - **Identitatea**
- Alte aspecte
  - **Autorizarea**
  - **Pierdere**
  - **Refuzul accesului (serviciilor)**

Securitate  
bazata pe criptografie





# Vulnerabilitati

- **Vulnerabilitate**  $\equiv$  slabiciune a unui sistem hard/software permite utilizatorilor neautorizati sa aiba acces asupra sa
  - Nici un sistem nu este 100% sigur
  - Vulnerabilitatile apar si datorita proastei administrari
- Tipuri:
  - permiterea refuzului serviciilor (**DOS – Denial Of Service**)
  - permiterea utilizatorilor locali cu privilegii limitate sa-si mareasca aceste privilegii fara autorizatie
  - permiterea utilizatorilor externi sa acceseze retea/sistemul local in mod neautorizat






# Vulnerabilitati

- Cauzele existentei vulnerabilitatilor
  - Bug-uri (erori) existente in programe, introduse deseori neintentionat
  - Ignorarea/nedocumentarea bug-urilor existente
  - Configurarea necorespunzatoare a programelor, serverelor si retelelor
  - Lipsa suportului din partea producatorilor (e.g. rezolvarea greoaie a bug-urilor)
  - Comoditatea sau necunoasterea problemelor de securitate de catre administratori de conducerea organizatiei





# Atacuri

- Cunoasterea **profilului atacatorului**
- Atribute ce trebuie considerate:
  - **Resursele disponibile**  
(financiare, tehnice,... + pregatirea in domeniu)
  - **Timpul alocat**  
(atacatorii rabdatori vor avea mai mult succes)
  - **Riscul asumat** – depinde de obiective  
(atacul ar putea fi revendicat sau nu de cracker)
  - **Accesul la Internet si calitatea acestuia**: tip (dial-up, conexiune satelit,...), mod de alocare a IP-ului,...
  - **Obiectivele urmarite** (recunoastere mondiala, denigrarea tinte, furt de informatii/bani etc.) 



# Atacuri

- Niveluri de atac
  - Oportunist
    - Scop “recreational”
    - Fara obiective/tinte clar definite
    - Se utilizeaza programe disponibile liber pentru a scana sau testa vulnerabilitati uzuale
    - Nu necesita acces in interiorul sistemului
    - Cunostinte vagi despre sistemul/organizatia tinta
    - Masuri de precautie:
      - ziduri de protectie (firewall-uri)
      - actualizarea versiunilor de programe





# Atacuri

- Niveluri de atac
  - Intermediar
    - Obiectiv conturat, la nivelul organizatiei
    - Se vor efectua aceleasi actiuni ca la atacul "recreational", dar se incearca ascunderea lor
    - Atacatorul are mai multa rabdare
    - Cunostinte tehnice mai profunde
    - Probabilitate mai mare de succes, posibil efecte mai puternice





# Atacuri

- Niveluri de atac
  - Sofisticat
    - Obiectiv foarte bine conturat
    - Tinta este de cele mai multe ori o organizatie
    - Atacurile pot trece peste masurile de prevedere
    - Atacatorul va avea multa rabdare
    - Se investeste timp pentru adunarea de informatii despre sistemul/organizatia tinta
    - Foarte bune abilitati tehnice
    - Probabilitate mare de succes





# Atacuri

- Tipuri de atac
  - **Accesul utilizator**
    - Atac prin acces via utilizator obisnuit sau cu privilegii superioare
    - Etape:
      - Colectarea de informatii – utilizatori, vulnerabilitati,...
      - Exploatarea
      - Deteriorarea
        - » Modificare de informatii
        - » Acces la date importante
        - » Asigurarea accesului ulterior la sistem
        - » Modificarea jurnalelor de sistem





# Atacuri

- Tipuri de atac
  - Accesul de la distanta la servicii-retea
    - Nu necesita acces utilizator la sistem
    - Creaza refuzuri de servicii prin cereri incorecte, eventual cu "caderea" serviciilor prost proiectate
    - Etape:
      - Colectarea de informatii – identificarea de servicii
      - Exploatarea – trimiterea de pachete la portul gasit
      - Deteriorarea
        - » Distrugerea unui serviciu de retea
        - » Defectarea/incetinirea (temporara) a unui serviciu sau a sistemului





# Atacuri

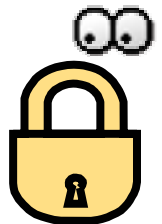
- Tipuri de atac
  - **Accesul de la distanta la diverse aplicatii**
    - Trimitere de date invalide aplicatiilor, nu serviciilor de retea (traficul nu e afectat)
    - Nu necesita obtinerea de acces utilizator
    - Etape:
      - Colectarea de informatii – identificarea aplicatiei (e.g. server sau client Web, aplicatie gen MS Office)
      - Exploatarea – trimiterea continutului, direct sau indirect (i.e. via e-mail), spre aplicatie
      - Deteriorarea
        - » Stergerea/copierea fisierelor utilizatorilor
        - » Modificarea fisierelor de configuratie





# Atacuri

- Tinta
  - Organizatii publice sau guvernamentale
    - Recunoastere in rindul cracker-ilor
    - Captarea atentiei mass-mediei
    - Revendicari etice, politice,...
  - Furnizori de servicii Internet
    - Sabotarea activitatii
  - Companii private
    - Discreditare
    - Furt de informatii
    - Razbunare din partea fostilor angajati
  - Persoane fizice
    - Cu scop recreational





# Atacuri

## • Moduri de atac

### – Bomba e-mail (e-mail bombing)

- Trimiterea repetata a unui mesaj (de dimensiuni mari) spre o adresa e-mail a unui utilizator
- Incetineste traficul, umple discul
- Unele atacuri pot folosi adrese e-mail multiple existente pe serverul tinta
- Se poate combina cu falsificarea adresei (e-mail spoofing)





# Atacuri

- **Moduri de atac**

- **Spam** (e-mail spamming)

- Trimiterea de mesaje nesolicitate (reclame)
    - Adresa expeditorului e falsa
    - Efectul atacului e accentuat  
daca mesajul este trimis pe o lista de discutii

- **Abonarea la liste de discutii**

- "Atac" ce determina enervarea victimei, facilitat de diverse programe disponibile in Internet
    - Cauzeaza trafic inutil de retea





# Atacuri

- **Moduri de atac**

- Falsificarea adresei expeditorului  
(e-mail spoofing)

- Folosita pentru ascunderea identit. expeditorului sau pentru determinarea utiliz. sa raspunda la atac ori sa divulge informatii (e.g. parole)
- Slabiciunea e datorata protocolului SMTP
- Utilizatorii trebuie educati sa nu raspunda expeditorilor necunoscuti si sa nu divulge informatii confidentiale





# Atacuri

## • Moduri de atac

### – Refuzul serviciilor (Denial Of Service)

- Degradeaza calitatea functionarii unor servicii sau conduce la dezafectarea lor
- **Bombardament cu pachete** (packet flood)
  - se trimite un numar mare de pachete spre o anumita gazda de la o singura sursa ori provenind de la **surse multiple** (Distributed DOS)
    - Segmente TCP (cu setarea SYN, ACK sau RST)
    - Pachete ICMP (ping flood)
    - Pachete UDP





# Atacuri

## • Moduri de atac

### – Refuzul serviciilor (Denial Of Service)

- Se poate falsifica adresa IP a expeditorului (IP spoofing)
- Se pot modifica porturile sursa/destinatia (pentru a trece de firewall-uri)
- Exemple
  - *SYN flood* – cereri multiple de realizare de conexiuni
  - *Ping of death* – atac cu pachete ICMP mari
  - *Teardrop* – exploatarea implementarilor TCP/IP care nu gestioneaza corect pachetele IP
  - *Smurf* – atac ICMP asupra adresei de broadcast





# Atacuri

- **Moduri de atac**

- **Depasirea capacitatii bufferelor**  
(buffer overflow)

- Unele programe pot aloca spatiu insuficient pentru unele date, depasirile survenite pot produce executarea de comenzi ca root
    - Uzual, atacul provine din interior, dar poate fi si din exterior (via un cal troian)





# Atacuri

- **Moduri de atac**

- **Interceptarea rețelei** (IP sniffing)

- Monitorizarea datelor care circula printr-o interfata de retea
  - se pot detecta parole transmise necriptate
- Atacul provine din interior
- Pentru rețele de viteză mare (100 M/s) unele pachete nu pot fi captate de **sniffer**
- Soft-ul de interceptare trebuie supravegheat
- Exemple: **tcpdump**, **Ethereal**





# Atacuri

- **Moduri de atac**

- **Cai troieni** (trojan horses)

- Programe rau intentionate, "deghizate" sub forma unor executabile utile
    - Apeleaza programe neautorizate sau sunt modificate, incluzind cod nelegitim
    - Actiuni: colectarea de informatii, distrugerea de informatii, lansarea de atacuri spre alte sisteme
    - Exemple: **sendmail** sau "vaduva neagra" (blocheaza sau corupe browsere Web)





# Atacuri

- **Moduri de atac**

- **Usi ascunse** (back doors / traps)

- Caz particular de cai troieni
    - Creaza o “poarta” (e.g. utilizator, port,...) care permite accesul ulterior la calculator si/sau cistigarea de privilegii

- **Viermi** (worms)

- Programe care se multiplica, transferindu-se pe alte calculatoare si efectuind distrugeri
    - Exemplu: Internet Worm (1988)



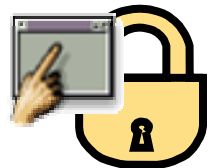


# Atacuri

- **Moduri de atac**

- Ghicirea parolelor (password guessing)

- Folosirea unui program ce determina parolele prost alese (prea simple)
      - Prea scurte, utilizeaza cuvinte de dictionar, numerice
    - Protectie prin **/etc/shadow**, reguli stricte de schimbare a parolelor, educarea utilizatorilor, folosirea de programe de tip **spargator de parole** (password cracker)





# Atacuri

## • Moduri de atac

### – Virusi

- Programe ce efectueaza operatii nedorite (distructive), cu capacitati de “multiplicare” – infectarea altor programe (uzual, executabile)
- Mai putin raspinditi in Unix/Linux, de obicei avind efect doar daca se executa sub auspicii de root
- Pot genera si e-mail bombing
- Remedii:  
utilizarea de antivirusi si porti de e-mail





# Prevenirea

- La ce nivel trebuie luate masuri de securitate?
  - Nivelul fizic: inhibarea ascultarii mediilor de transmisie, interzicerea accesului fizic la server,...
  - Nivelul leg. de date: criptarea legaturii
  - Nivelul retea: ziduri de protectie (firewall-uri)
  - Nivelul transport: criptarea conexiunilor
  - Nivelul aplicatie: monitorizare si actualizare a soft-ului, jurnalizare, educare a utilizatorilor, politici generale adoptate,...





# Prevenirea

- Elaborarea de politici de securitate
  - Planificarea cerintelor de securitate
    - Confidentialitate, integritate, disponibilitate, control
  - Evidentierea riscurilor
  - Analiza raportului cost-beneficii
    - Costurile prevenirii, refacerii dupa dezastru etc.
  - Stabilirea politicilor de securitate
    - Politica generala (nationala, organizationala,...)
    - Politici separate pentru diverse domenii protejate
    - Standarde & reglementari (recomandari)
- Masurile luate pot fi tehnice si non-tehnice





# Prevenirea

- Elaborarea de politici de securitate – exemplu
  - Gestionarea accesului (nume de cont, alegerea si modul de schimbare a parolelor, blocarea terminalului, politica de acces din exterior,...)
  - Clasificarea utilizatorilor (grupuri, permisiuni, utilizatori speciali, utilizatori administratori,...)
  - Accesul la resurse (drepturi de acces la fisiere, directoare, criptarea fisierelor importante,...)
  - Monitorizarea activitatii (fisiere de jurnalizare)
  - Administrarea copiilor de siguranta (tipuri de salvari, medii de stocare, durata pastrarii,...)





# Supravietuirea

- **Supravietuirea**  $\equiv$  capacitatea unui sistem (calculator/retea) de a-si indeplini misiunea, in timp util, in prezenta atacurilor, defectelor sau accidentelor
- **Atac**  $\equiv$  eveniment potential distrugator provocat intentionat de persoane rau-voitoare
- **Defect**  $\equiv$  eveniment potential distrugator cauzat de deficiente ale sistemului sau ale unui factor de care depinde sistemul (e.g. defecte hard, bug-uri soft, erori ale utilizatorilor)
- **Accident**  $\equiv$  evenimente aleatoare (neprevazute); exemple: dezastre naturale, caderi de tensiune





# Supravietuirea

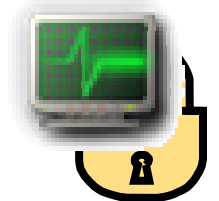
- Sistemul trebuie sa-si duca pina la capat misiunea chiar daca unele componente sau parti din sistem sunt afectate ori scoase din uz
- Sistemul trebuie sa sustina macar indeplinirea **functiilor vitale** (mission-critical)
  - Identificarea serviciilor esentiale
- Proprietati ale sistemului:
  - **Rezistenta la atacuri**
  - **Recunoasterea atacurilor si efectelor lor**
  - **Adaptarea la atacuri**





# Supravietuirea

- Instrumente sub Linux (Unix):
  - Utilitare de retea: ping, traceroute, netstat, ifconfig, route, host, finger, last, telnet
  - Scanere de porturi: NMAP
  - Interceptoare de retea: tcpdump, ethereal
  - Testarea securitatii locale: /etc/shadow, Crack, Titan
  - Verificari asupra sist. de fisiere: tripwire, showmount
  - Salvari de siguranta: tar, dump, amanda
  - Verificarea daemonilor: chkconfig
  - Protectia TCP/IP: iptables (firewall), sysctl, activarea mecanismului SYN cookies in nucleu





# Rezumat

- Preambul
- Vulnerabilitati
- Atacuri
- Prevenirea
- Supravietuirea





**Mulumiri pentru atentia acordata!**

