

Securitatea sistemelor informatice

C-02

Universitatea “Transilvania” din Brasov

Lect.dr. Costel ALDEA

Sisteme IT și probleme de securitate

- Sisteme informatice: disponibilitate și control
- Rețele de calculatoare
- Protocoale în Internet
- Viruși, viermi și troieni
- Amenințări și criterii de securitate

Amenințări în rețele de calculatoare

- ❑ Interceptare neautorizata, Modificare si distrugerea informațiilor

Citirea datelor din fișier sau baza de date, reluarea datelor, spionaj de parole, distrugere vizata de date si programe.

- ❑ Acces neautorizat la sisteme, folosirea resurselor unor componente de sistem sau de servicii de sistem sau interferarea cu disponibilitatea acestora

Manipularea datelor externe, blocarea conexiunilor pentru a bloca accesul persoanelor autorizate la date, folosirea unei platforme "sparte" pentru intruziuni suplimentare, obținerea drepturilor de acces, crearea unei identități false.

- ❑ Erori de software și de configurație

Profitând de punctele slabe de protocol si serviciile configurate incorect, reușesc programele malware sa se instaleze (viermi, viruși, troieni etc.)

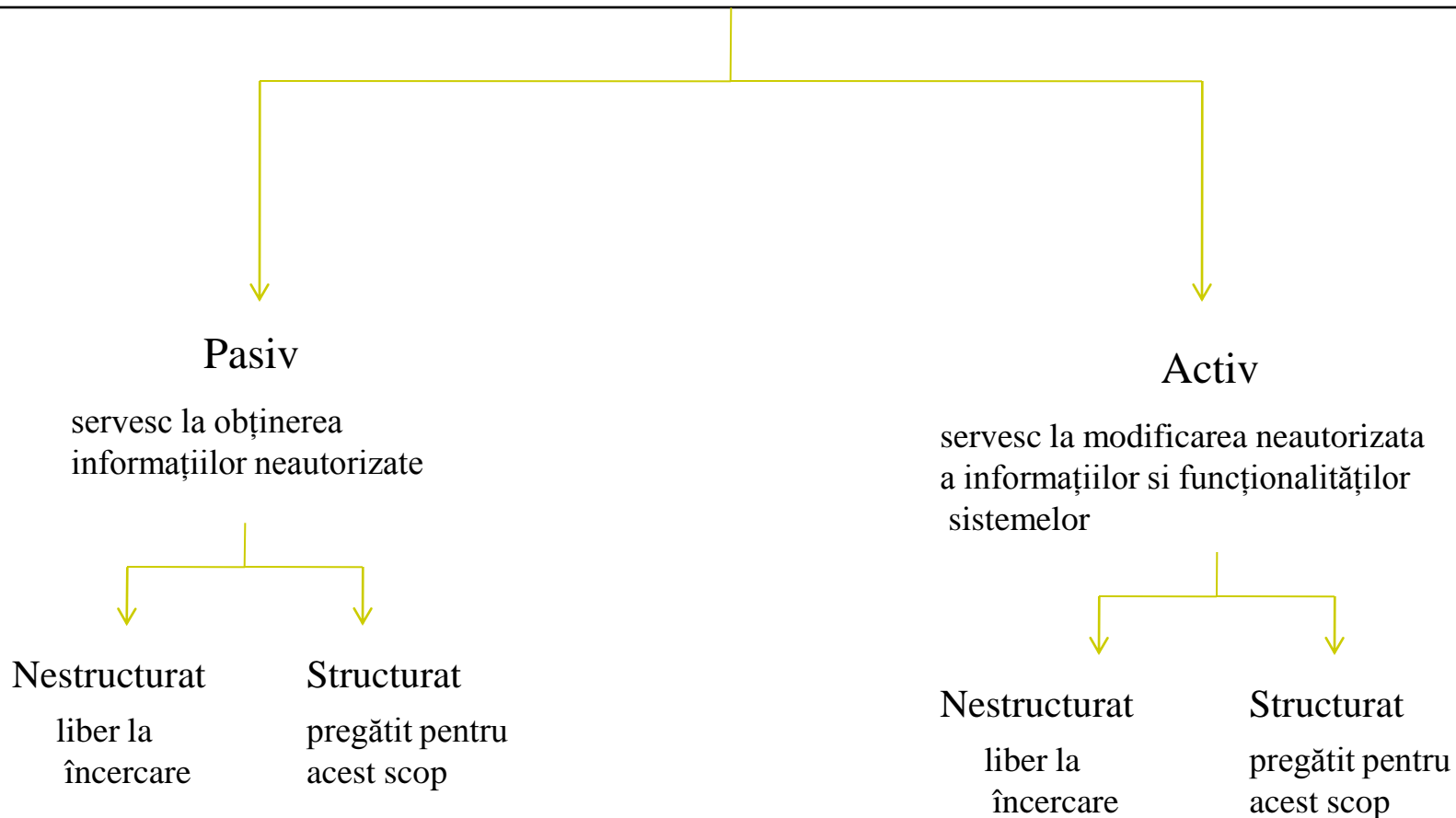
- ❑ Acces neautorizat la sistemele informatice

Eludarea controlului de acces la clădiri, cabluri si consumabile.

- ❑ Forte majore

Cum ar fi fulger, dezastre ecologice, pana de curent.

Atacuri în rețele de calculatoare



Atacurile pot veni atât din interior cât și exterior.

Atacuri în rețele de calculatoare, diverse scenarii

- ❑ Sniffing-Attack: interceptarea neautorizata a informațiilor (pasiv)
- ❑ Spoofing-Attack: simularea unei identități false, denumit și “Masquerade” (activ)
- ❑ Denial-of-Service-Attack: afectează disponibilitatea sistemului sau a serviciului, numita si inundarea-înfundarea resurselor (activ)
- ❑ Social Engineering-Attack: acțiuni de către persoanele neautorizate. De exemplu interogarea parolei prin telefon simulând o situație de urgenta.

Atacuri în rețele de calculatoare, varietate de motive

- ❑ Spionaj industrial profesional/Crima organizata

Un domeniu de activitate ridicata, servicii de informatii internationale, structuri mafioate, persoane echipate cu cunostiinte necesare, lacomie.

- ❑ Hackeri curiosi

Vanitate, dorinta de experimentare, nivel de expertiza inalta si timp liber, de obicei cu prejudiciu neintentionat


- ❑ Vandalism


Hackeri agresivi, organizatie criminala cu scop de distrugere, motivatie politica.


- ❑ Fostii sau curentii angajati

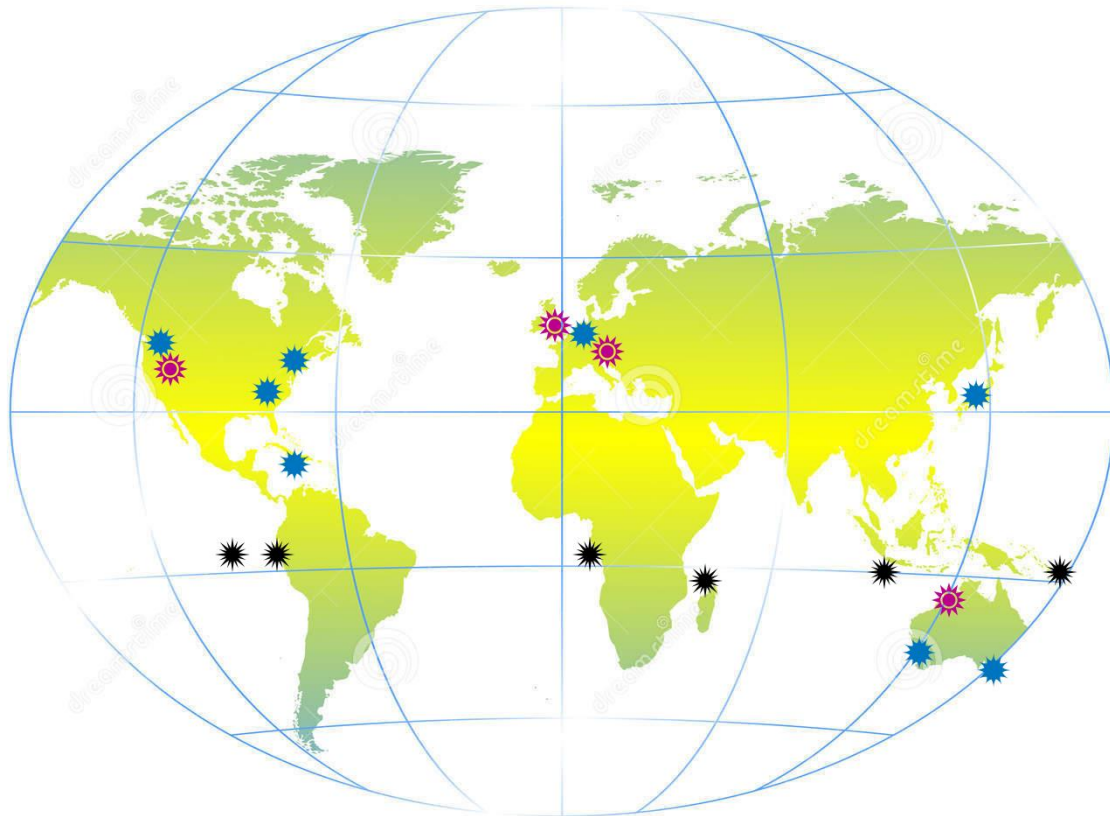
Frustrare, razbunare pentru concediere, imbogatire financiara, cunostiinte ridicate despre interiorul companiei, acces la terminale.

Spionaj economic și industrial

 Sisteme de monitorizare
pentru Intelsat și alți sateliți

 satelit de telecomunicații
internaționale

 Stație de control pentru
sateliți de recunoaștere





Stație de spionaj Misawa Base, Japan



Stație de spionaj Bad Aibling, Germania

Amenințări de atacuri asupra :

Confidențialitatea datelor

Sniffing-Attacks

→ Spionaj de informații discrete(ISP, router, sniffing, scanare de porturi, troieni, etc.)

Integritatea datelor

Spoofing-Attacks

→ Prezentând informații false(Mail, DNS, IP, ARP, Spoofing, etc.)

Răspunderea asupra datelor

Spoofing-Attacks

→ Pretinzând identitate falsă(PIN sniffing cu DNS-Spoofing, LAN-Sniffing cu ARP-Spoofing)

Disponibilitatea sistemului

Denial-of-Service-Attacks

→ Prăbușirea funcționalității sistemului (Mail-bombing, SYN-flood, UDP-flood, Ping-of-death-attack)

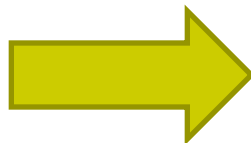
Controlul accesului la sistem

Spoofing-Attacks

→ Accesul la servicii de sistem interzise (NFS-Spoofing, spargerea parolei)

Situația: transmisii de date si protocoale incerte

Vulnerabilitățile
sunt diverse



Amenințările
sunt diverse

- ❑ Punctele slabe a protocoalelor TCP/IP
- ❑ Punctele slabe a serviciilor de aplicare TCP/IP
- ❑ Erori de software
- ❑ Erori de configurație

- ❑ Interceptarea mesajelor
- ❑ Schimbarea mesajului
- ❑ Aflarea mesajului
- ❑ Interceptarea si ascultarea mesajului
- ❑ Reluarea mesajului

Scop securitate: metoda sigură a transmiterea datelor !!!

Vulnerabilități ale rețelelor de calculatoare

(A) Topologie de rețea

□ Interceptarea nodurilor de rețea

Computer: un amestec de semnaluri complexe, prin urmare este greu de exploatat.

Terminale: radiații puternice(semnal pana la 1,5km chiar si prin pereți din beton armat) astfel este ușor de interceptat în special de ecrane TFT(amperaj mare)

Printer: unele tipuri pot fi ușor interceptate(ex. imprimanta daisy-wheel)

Placi,Server: greu de interceptat

□ Interceptarea cablajului LAN

Ethernet: toata informația (circulă) este într-un singur cablu, în Thickwire și poate fi exploatată fără separare; în Thinwire separarea este necesară; când nu avem o punte în sine prizele sunt disponibile

Token-Ring: monitorizarea logica asupra unui nod suplimentar este făcut de către un nod vecin

FDDI: chiar si cablul de fibra optica poate fi interceptat însă monitorizarea unui nod logic necesita acces fizic la un concentrator.

Punctele slabe ale rețelelor de calculatoare

(A) Topologie de rețea

❑ Interceptarea în WAN

Linii închiriate: pot fi interceptați de către gestionarii cablului, intruziunea nodurilor de rețea din extern este exclusă

Unde radio: este datorată vitezei de transmisie reduse, ușor de interceptat

❑ Topologia stea

Huburile distribuie informații de la fiecare intrare până la ieșirea switchului, transmite informația doar la calculatorul țintă.

❑ Topologia bus

Fiecare primește semnalul de la calculatorul care trimite, transmitătorul nu știe dacă destinatarul a primit datele.

Punctele slabe ale rețelelor de calculatoare

(A) Topologie de rețea

□ Noduri intermediare (routere)

Calculatoare care înțeleg protocolul de rețea, asigură pentru ambele rețele o interfață, divizarea mesajelor, transmiterea părților de mesaje pe căi diferite, pierderea de mesaje, prin urmare destinatarul primește doar părți din mesaj sau mesajul în ordinea greșită.

□ Modem

Conversia semnalelor digitala in analoga si vice-versa, transmiterea informațiilor prin rețeaua de telefonie.

PC-ul cu un modem poate trimite date ocolind Firewall-ul.

Punctele slabe ale rețelelor de calculatoare TCP/IP

(B) Familii de protocoale

□ IP-Spoofing

Protocoalele IP nu verifică sursa și destinația adresei pachetelor de date, astfel autentificarea partenerului de comunicare nu este posibilă și adresele nu pot fi falsificate. Un hacker folosește adresa IP a victimei într-o rețea străină ca adresă sursă pentru a trimite date sub formă de pachete ale unui calculator intern.

□ ARP-Spoofing

Spionaj de informații dintr-o rețea LAN prin manipularea cache-ului ARP. Sunt trimise pachete de date la calculatorul țintă. Hackerul trimite un "răspuns" ARP cu adresa lui de hardware și adresa IP a victimei la un calculator din rețeaua LAN care salvează răspunsul în memoria cache.

Punctele slabe ale rețelelor de calculatoare TCP/IP

(B) Familii de protocoale

□ DNS-Spoofing

Anumite servicii folosesc servere DNS pentru atribuirea numelui de domeniu la adresele IP. Hackerul manipulează baza de date a unui server DNS pentru a atribui adresa lui de IP unui alt calculator, astfel calculatorul victimă are încredere în acest calculator (de exemplu numele de domeniu este inclus în fișierul Trusted Host), astfel hackerul poate accesa calculatorul victimei cu un apel rlogin (autentificare de la distanță). În versiunile mai vechi ale software-ului DNS hackerul putea intra ca un Man-in-the-Middle în comunicarea dintre client și server, deoarece serverul DNS citește date în memoria cache care nu au fost solicitate.



Punctele slabe ale rețelelor de calculatoare TCP/IP

(B) Familii de protocoale

□ TCP-atack prin numere de secventa

Acest tip de attack foloseste punctele slabe a implementarii Unix-ului cu un contor simplu, acesta creste in mod regulat si fiecare mesaj primeste numarul curent. TCP asigura ca toate datele au sosit si trimite confirmare. Se initieaza o conexiune pe un port si primeste in confirmare numarul de ordin. Apoi preia identitatea unui calculator victima si initieaza o conexiune la server prin acest port. Raspunsul ajunge la calculatorul victima insa hackerul poate calcula acum numarul de ordine, astfel a deghizat calculatorul victima. Serverul vede doar ca a facut o conexiune cu calculatorul victima.

Punctele slabe ale rețelelor de calculatoare TCP/IP

(B) Familii de protocoale

□ TCP-SYN-flood attack

Acest atac profita de slăbiciunile unității de conectare TCP. Hackerul trimite un număr mare de pachete SYN pe calculatorul victima, în timp ce el folosește adrese de expeditor inexistentă. Răspunsurile verificate ajung pe adresa falsă, iar calculatorul victimă așteaptă în zadar pentru confirmarea expeditorului. Calculatorul este încetinit din această cauză și în cele din urmă cedează.

□ UDP protocol

UDP nu conține informații cu privire la inițiatorul unei conversații astfel încât un Firewall nu poate determina dacă un pachet UDP vine din interior sau exterior. UDP mai este folosit de către aplicații cum ar fi: DNS, RIP, RADIUS, TFTP, SNMP.

□ Modificarea tabelului de rutare din router

Prin abuzul protocolului RIP poate hackerul să transmită informații în propriul său calculator.



Punctele slabe ale rețelelor de calculatoare TCP/IP

(B) Familii de protocoale

□ FTP

La un server FTP anonim se pot conecta mai mulți clienți (fără parolă și autentificare), astfel datele publice nu pot fi modificate.

FTP in modul activ: Sistemul recunoaște crearea clientului și asigură o conexiune la portul dorit deci firewall-ul trebuie să aprobe toate conexiunile din afara rețelei, ca să nu fie descoperit portul. Doar în modul pasiv permite FTP-ul serverului să stabilească conexiunea la port.

□ Mail-Spoofing

Folosind SMTP mesajele sunt transmise și stocate liber și neprotejat. De asemenea nu sunt protejate nici datele expeditorului. Hackeri pot intercepta datele trimise, pot să schimbe sau să manipuleze mesajul expeditorului.



Punctele slabe ale rețelelor de calculatoare TCP/IP

(B) Familii de protocoale

□ Cookies

Schimbul de date a fost efectuată cu ajutorul cookie-urilor între client și server, se execută automat în fundal, poate fi vizualizat dar nu și controlat.

Serverul poate urmări clientul pe internet până la informațiile despre profilul lui.

□ JavaScript

Se folosește în scopuri de a edita și vizualiza pagini HTML prin intermediul browserului clientului, de aici apar multe probleme de securitate.

□ Cod mobil

Pe de o parte poate fi vizualizat și modificat în timpul transportului pe de altă parte poate fi executat pe calculatorul oaspete.

Criterii de securitate

caracteristici pe care un sistem IT trebuie să le asigure.

Confidențialitate



codare

→ Datele dintr-un mesaj nu pot fi accesate de un "third party"

Integritate



functia hash

→ Mesajul rămâne neschimbat

Autenticitate



semnături digitale, autentificare

→ Creatorul unui mesaj este identificat in mod clar si originea mesajului nu poate fi negat

Disponibilitate



redundanta, proceduri de back-up

→ Pentru a evita defecțiuni ale sistemului informatic

Non-repudiarea



semnături digitale, PKI, certificate

→ Transmițătorul și receptorul nu pot nega trimiterea sau primirea unui mesaj

Control de acces



technici de autentificare

→ Doar persoane identificate si autorizare au acces la date de resurse

Cerințe de securitate



pentru a determina gradul de

confidențialitate

integritate

autenticitate

disponibilitate

non-repudiare

control de acces



realizat

Conceptul de securitate

Intrebări

