

Sisteme IT si probleme de securitate

- Sisteme informatice: disponibilitate si control
- Retele de calculatoare
- Protocoale in Internet
- Virusi, viermi si troieni
- Amenintari si criterii de siguranta



Amenintari in retele de calculatoare

- ❑ Interceptare neautorizata, Modificare si distrugerea informatiilor

Citirea datelor din fisier 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, obtinerea drepturilor de acces, crearea unei identitati false.

- ❑ Erori de software si de configuratie

Profitand de punctele slabe de protocol si serviciile configurate incorect, reusesc programele malware sa se instaleze (viermi, virusi, troieni etc.)

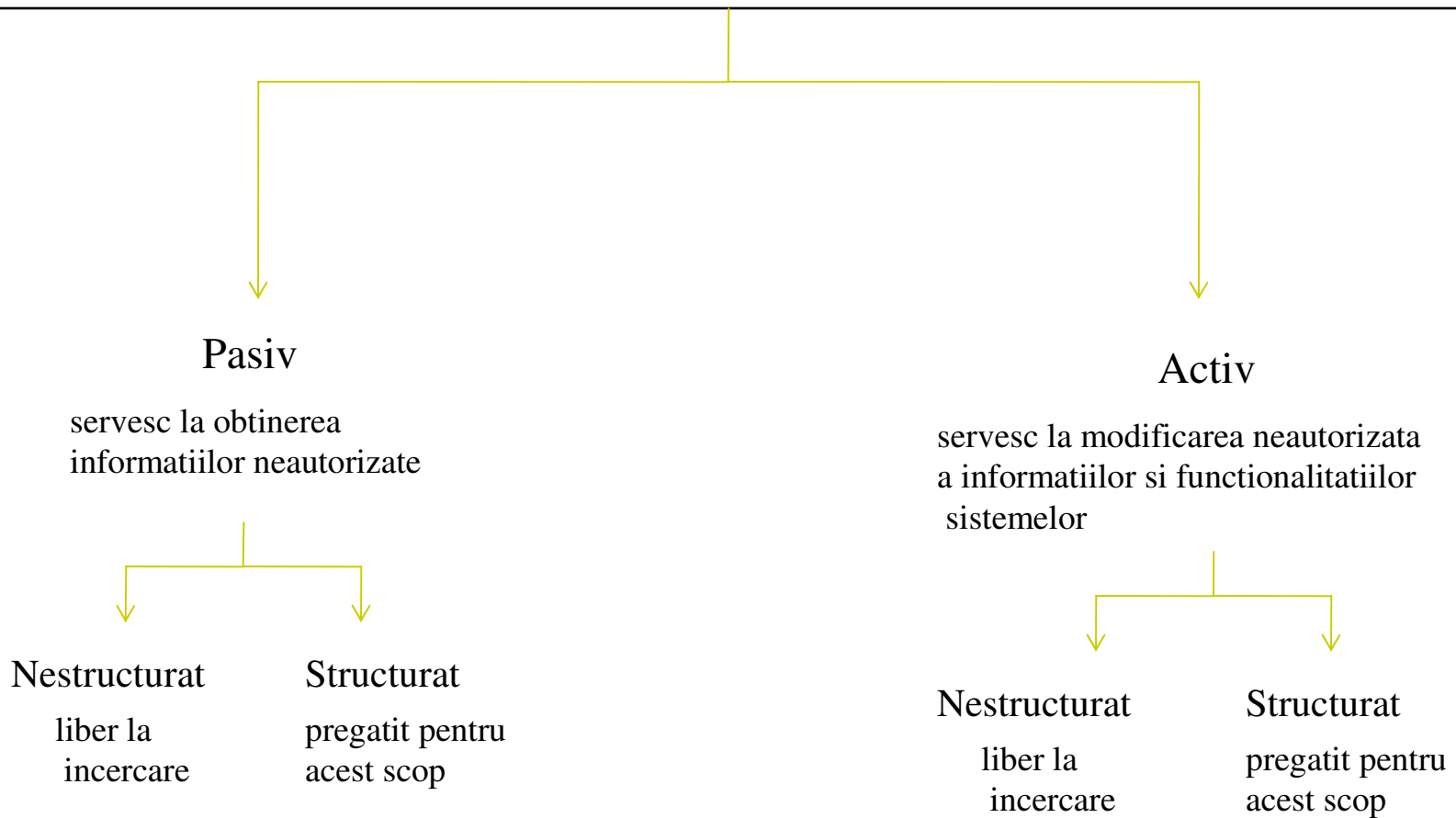
- ❑ Acces neautorizat la sistemele informatice

Eludarea controlului de acces la cladiri, cabluri si consumabile.

- ❑ Forte majore

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

Atacuri in retele de calculatoare





Atacuri in retele de calculatoare, diverse scenarii

- ❑ Sniffing-Attack: interceptarea neautorizata a informatiilor (pasiv)
- ❑ Spoofing-Attack: simularea unei identitati false numita si "Masquerade"(activ)
- ❑ Denial-of-Service-Attack: afecteaza disponibilitatea sistemului sau a serviciului, numita si infundarea resurselor (activ)
- ❑ Social Engineering-Attack: actiuni de catre persoanele nautorizate. De exemplu interogarea parolei prin telefon simuland o situatie de urgenta.



Atacuri in retele de calculatoare, varietate de motive

- ❑ Spionaj industrial profesional/Crima organizata

Un domeniu de activitate ridicata, servicii de informatii internationale, structuri mafiotie, 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

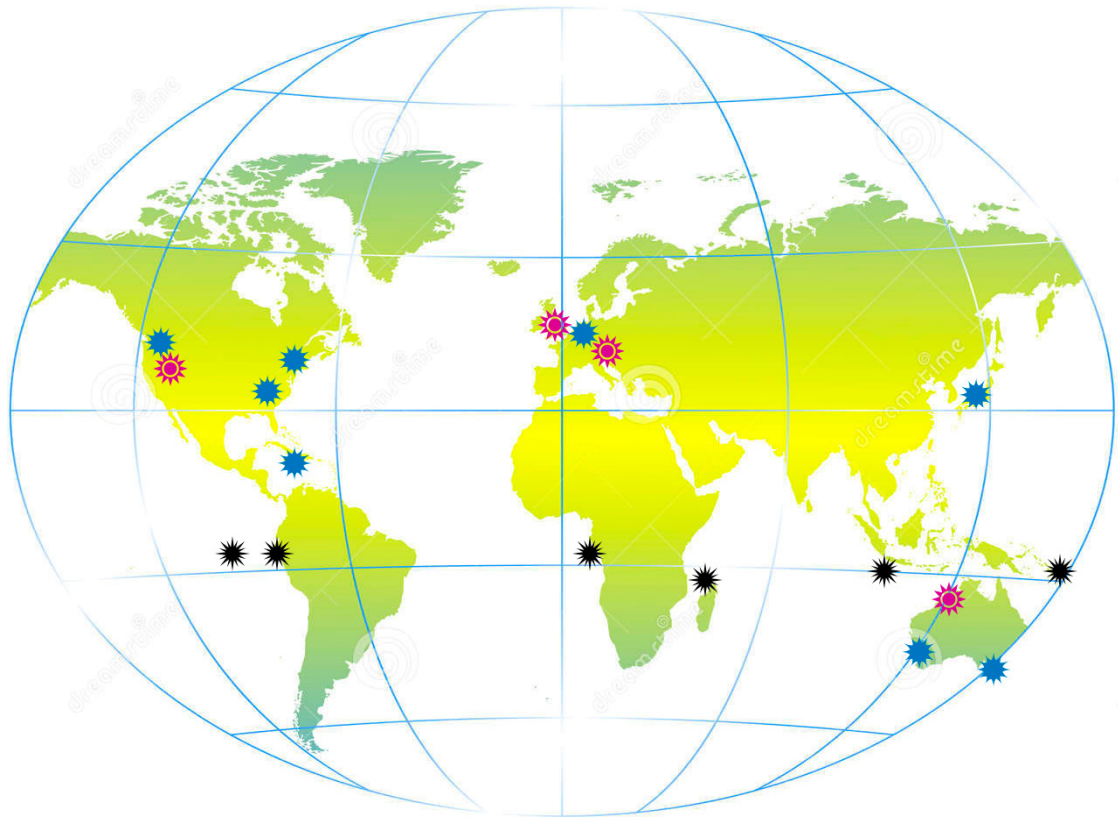
Frustrare, razbunare pentru concediere, imbogatire financiara, cunostiinte ridicate despre interiorul companiei, acces la terminale.

Spionaj economic si industrial

 Sisteme de monitorizare
pentru Intelsat si alti sateliti

 satelit de telecomunicatii
internationale

 Statie de control pentru
sateliti de recunoastere





Statie de spionaj Misawa Base, Japan



Statie 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 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-to-death-attack)

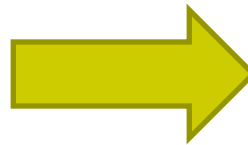
Controlul de acces al sistemului

Spoofing-Attacks

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

Situatia: transmisii de date si prtocoloale incerte

Vulnerabilitatile
sunt diverse



Amenintarile
sunt diverse

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

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

Scop securitate: metoda sigura a transmiterea datelor !!!

Vulnerabilitati ale retelelor de calculatoare

(A) Topologie de retea

□ Interceptibilitatea nodurilor de retea

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

Terminale: radiatii puternice(semnal pana la 1,5km chiar si prin pereti din beton armat) astfel este usor de interceptat in special de ecrane TFT(amperaj mare)

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

Placi,Server: greu de interceptat

□ Interceptarea cablajului LAN

Ethernet: toata informatia este intr-un singur cablu, in Thickwire poate fi exploatat fara separare, in Thinwire separarea este necesara, cand nu avem o punte in sine prizele sunt disponibile

Token-Ring: monitorizarea logica asupra unui nod suplimentar este facut de catre un nod vecin

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



Punctele slabe ale retelelor de calculatoare

(A) Topologie de retea

□ Interceptarea in WAN

Linii inchiriate: pot fi interceptati de catre gestionatorii cablului, intruziunea nodurilor de retea din extern este exclusa

Unde radio: este datorata vitezei de transmisie reduse, usor de interceptat

□ Topologia stea

Huburile distribuie informatii de la fiecare intrare pana la iesirea switchului, transmite informatia doar la calculatorul tinta.

□ Topologia bus

Fiecare primeste semnalul de la calculatorul care trimite, transmitatorul nu stie daca destinatarul a primit datele.



Punctele slabe ale retelelor de calculatoare

(A) Topologie de retea

□ Noduri intermediare (routere)

Calculatoare care inteleg protocolul de retea, asigura pentru ambele retele o interfata, divizarea mesajelor, transmiterea bucatilor de mesaje prin cai diferite, pierderea de mesaje, prin urmare destinatarul primeste doar parti din mesaj sau mesajul in ordinea gresita.

□ Modem

Conversia semnalelor digitala in analoga si vice-versa, transmiterea informatiilor prin reseaua de telefonie.

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



Punctele slabe ale retelelor de calculatoare TCP/IP

(B) Familii de protocoale

□ IP-Spoofing

Protocoalele IP nu verifica sursa si destinatia adresei pachetelor de date, astfel autentificarea partenerului de comunicare nu este posibila si adresele nu pot fi falsificate. Un hacker foloseste adresa IP a victimei intr-o retea straina ca adresa sursa pentru a trimite date sub forma de pachete ale unui calculator intern.

□ ARP-Spoofing

Spionaj de informatii dintr-o retea LAN prin manipularea cach-ului ARP. Sunt trimisi pachete de date la calculatorul tinta. Hackerul trimite un "raspuns" ARP cu adresa lui de hardware si adresa IP a victimei la un calculator din retea LAN care salveaza raspunsul in memoria cache.



Punctele slabe ale retelelor de calculatoare TCP/IP

(B) Familii de protocoale

□ DNS-Spoofing

Anumite servicii folosesc servere DNS pentru atribuirea numelui de domeniu la adresele IP. Hackerul manipuleaza baza de date a unui server DNS pentru a atribui adresa lui de IP la un alt calculator, astfel calculatorul victima are incredere in acest calculatorul(de exemplu numele de domeniu este inclusa in dosarul Trusted Host Datei), astfel poate hackerul cu un apel rlogin(authenticare de la distanta) accesa calculatorul victimei. In versiunile mai vechi ale software-ului DNS hackerul putea intra ca un Man-in-the-Midle in comunicarea intre client si server, deoarece serverul DNS citește date in memoria cache care nu a fost solicitat. Clientul introducand un PIN iar hackerul intercepteaza acest lucru(PIN-Sniffing).



Punctele slabe ale retelelor 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 retelelor de calculatoare TCP/IP

(B) Familii de protocoale

□ TCP-SYN-flood attack

Acest atac profita de slabiciunile unitatii de conectare TCP. Hackerul trimite un numar mare de pachete SYN pe calculatorul victima, in timp ce el foloseste adrese de expeditor inexistentă. Raspunsurile verificate ajung pe adresa falsa iar calculatorul victima asteapta in zadar pentru confirmarea expeditorului. Calculatorul este incetinit din cauza aceasta si in cele din urma cedeaza.

□ UDP protocol

UDP nu contine informatii cu privire la initiatorul unei conversatii astfel incat un Firewall nu poate determina daca un pachet UDP vine din interior sau exterior. UDP mai este folosit de catre aplicatii cum ar fi: DNS, RIP, RADIUS, TFTP, SNMP.

□ Modificarea tabelelor de routare din router

Prin abuzul protocolului RIP poate hackerul sa transmita informatii in propriul sau calculator.



Punctele slabe ale rețelelor de calculatoare TCP/IP

(B) Familii de protocoale

□ FTP

La un server FTP anonim se pot conecta mai multi clienti(fara password si autentificare), astfel datele publice nu pot fi modificate.

FTP in modul activ: Sistemul recunoaste crearea clientului si asigura o conexiune la portul dorit deci firewal-ul trebuie sa aprobe toate conexiunile din afara rețelei, ca sa nu fie descoperit portul. Doar in modul passiv permite FTP-ul serverului sa stabileasca conexiunea la port.

□ Mail-Spoofing

Cum SMTP mailurile sunt transmise si stocate liber si neprotejat. De asemenea nu sunt protejate nici datele expeditorului. Hackeri pot intercepta datele trimise, poate sa schimbe sau sa 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 siguranță

caracteristici pe care un sistem IT trebuie să le asigure.

Confidentialitate



codare

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

Integritate



funcția hash

→ Mesajul rămâne neschimbat

Autenticitate



semnături digitale, autentificare

→ Creatorul unui mesaj este identificat în mod clar și originea mesajului nu poate fi negat

Disponibilitate



redundanță, proceduri de back-up

→ Pentru a evita defecțiuni ale sistemului informatic

Nonrepudierea



semnături digitale, PKI, certificate

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

Control de acces



tehnici de autentificare

→ Doar persoane identificate și autorizate au acces la date de resurse

Cerinte de siguranta



pentru a determina gradul de

confidentialitate

integritate

autenticitate

disponibilitate

nonrepudiere

control de acces



realizat

Conceptul de securitate