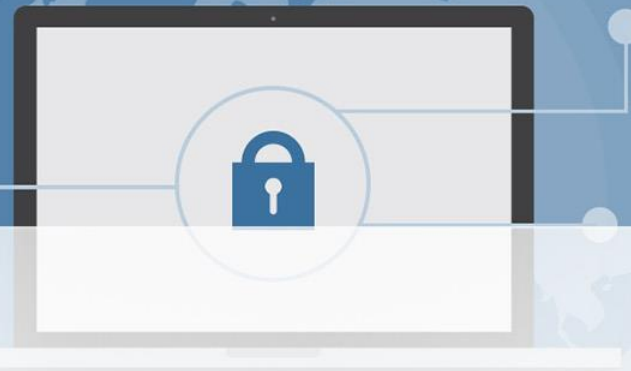
Criptografie și Securitate Cibernetică

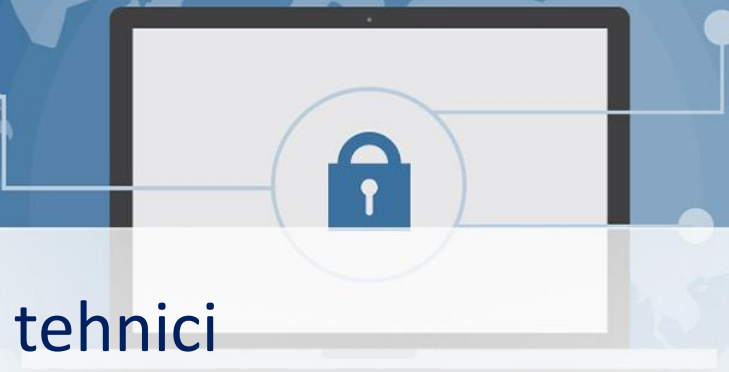
RCC - CSC 7

Conținut



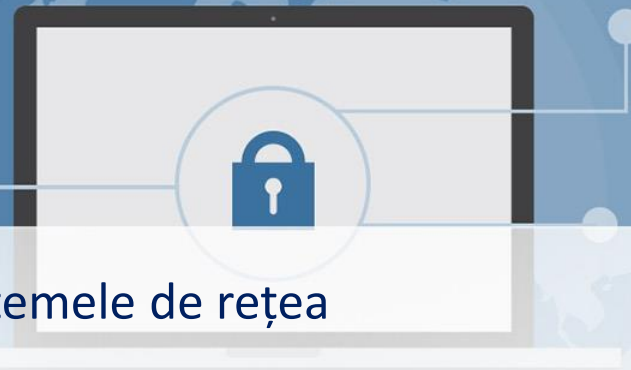
- Intruziuni și Intruși
  - Comportamente și tehnici
  - Detectarea intruziunilor
  - Gestionarea parolelor
- Software rău intenționat
  - Tipuri de software rău intenționat
  - Viruşi
  - Contramăsuri pentru viruși
  - Viermi
  - Atacuri Denial of Service distribuite

Intruziuni și Intruși



- Comportamente și tehnici
- Detectarea intruziunilor
  - Detectare statistică
  - Detectarea bazată pe reguli
- Gestionarea parolelor

Intruziuni și Intruși

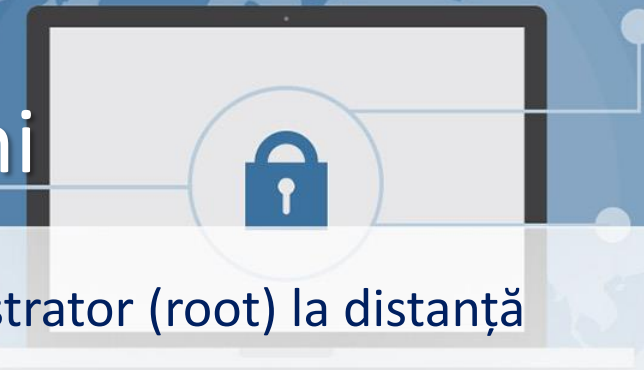


- Problemă semnificativă pentru sistemele de rețea
  - de accesul ostil sau nedorit
  - fie prin rețea, fie local
- Pot identifica clasele de intruși:
  - mascat (o persoana neautorizată care folosește contul unei persoane autorizate din sistem)
  - răufăcător (un utilizator din sistem care folosește resurse la care accesul nu îi este autorizat)
  - utilizator clandestin (un individ care deține drepturi de supracontrol și le folosește pentru a evita mecanismele de control
- Diferite niveluri de competență

Intruders

- În mod clar o problemă în creștere
  - de la "Wily hacker" în 1986/87
  - la escaladarea în mod clar a statisticilor CERT
- Nivel
  - Ușor: explorare, costuri legate de consumul de resurse
  - Grav: acces/modificare date, perturbă sistemul
- Dezvoltarea de CERTs (Computer Emergency Response Teams)
- Tehnicile de intruziune și modele de comportament sunt în continuă schimbare

Exemple de intruziuni

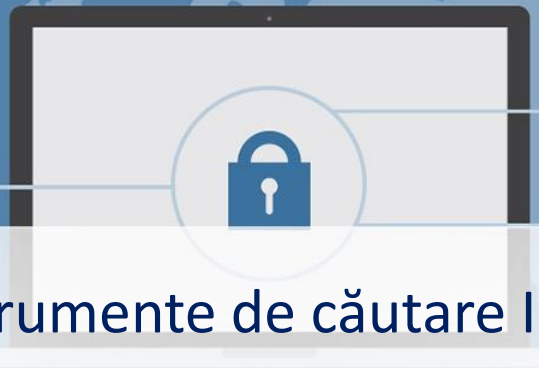


- Compromitere utilizator administrator (root) la distanță
- Modificare server web
- Identificare/spargere parole
- Copierea vizualizării datelor/bazelor de date sensibile
- Rularea unui sniffer de pachete
- Distribuirea de software piratat
- Utilizarea unui echipament nesecurizat pentru a accesa resurse
- Înlocuirea unui utilizator pentru a reseta parola
- Utilizarea unei stații de lucru nesupravegheată

Hackeri

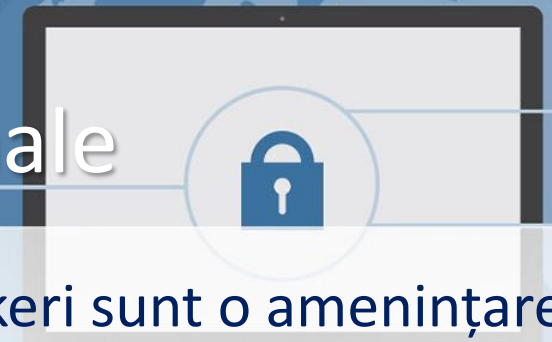
- Motivați de plăcerea accesului neautorizat și de statutul dat de activitate
  - comunitatea se bazează pe meritocrație
  - statutul este determinat de nivelul de competență
- Intruziunile de nivel ușor ar putea fi tolerate
  - consumă resurse și pot încetini performanța
  - nu se știe în prealabil nivelul de intruziune (ușor/grav)
- Sistemele IDS/IPS/VPN pot ajuta la contracararea atacurilor
- Conștientizarea problemei a condus la înființarea de CERTs
  - colectează/difuzează informații vulnerabilități /răspunsuri la atacuri

Exemplu de comportament hacker



1. Selectare țintă utilizând instrumente de căutare IP
2. Scanare rețea pentru identificare servicii accesibile
3. Identificarea serviciilor potențial vulnerabile
4. Identificare parole (Brute Force)
5. Instalare instrument de administrare la distanță
6. Urmărește autentificarea de utilizatori cu drepturi de administrare pentru le captura parola
7. Utilizarea parolei pentru a accesa restul rețelei

Organizații infracționale

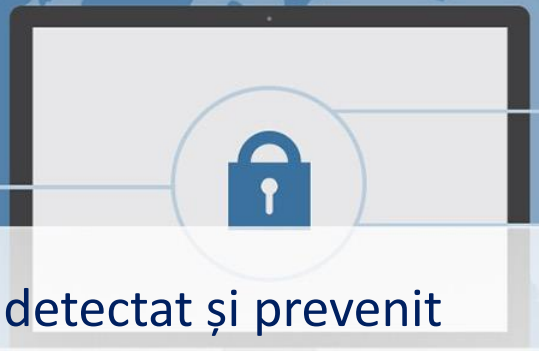


- Grupurile organizate de hackeri sunt o amenințare
  - pot proveni din corporații/instituții/grupuri neafiliate
  - de obicei tineri
  - de multe ori din țări est-europene sau Rusia
  - o țintă predilectă sunt cardurile de credit, comerț online
- Hackerii criminali au, de obicei, obiective specifice
- Odată penetrat un sistem, acționează rapid și pleacă
- Sistemele IDS/IPS ajuta, dar sunt puțin eficiente
- Datele sensibile necesită o protecție puternică

Comportament infracțional

1. acționează rapid și precis pentru a-și face activitățile mai greu de detectat
2. exploatează sistemul prin porturile vulnerabile
3. folosește cai troieni (software ascuns) pentru a lăsa porți (back doors) pentru re-intrare
4. utilizează aplicații sniffer pentru a captura parole
5. nu rămâne în sistem până va fi observat
6. face puține greșeli sau deloc.

Atacuri din interior

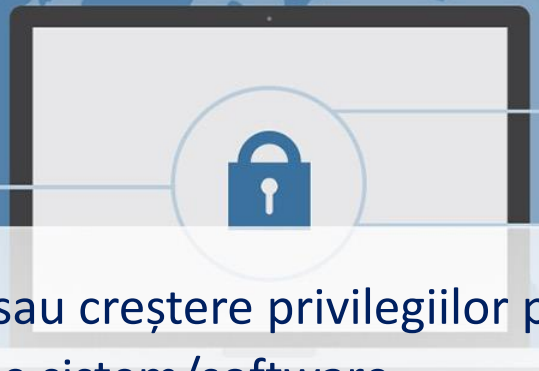


- dintre cele mai dificile atacuri de detectat și prevenit
- angajații au acces și cunoștințe privind sistemele
- poate fi motivat de răzbunare/privilegii
  - atunci când este reziliat un contract de muncă
  - preluarea datelor clienților atunci când trece la concurent
- Sistemele IDS/IPS pot ajuta, dar e nevoie și de:
  - Alocarea celui mai mic privilegiu necesar, monitorizare jurnalele de evenimente, autentificare puternică, procedură clară la terminarea contractelor de munca pentru a blocare accesul în rețea, copierea/ștergerea datelor de pe discuri înainte de reutilizare

Exemplu de comportament din interior

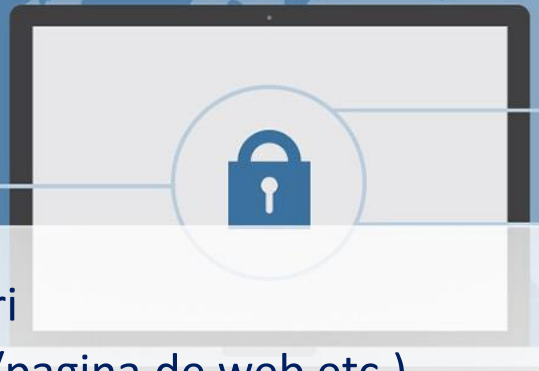
1. crearea de conturi de rețea pentru ei înșiși și prietenii lor
2. conturi de acces și aplicații pe care nu le-ar utiliza în mod normal pentru munca lor zilnică
3. trimiterea de e-mail-uri foștilor și potențialilor angajatori
4. efectuarea de sesiuni de mesagerie ascunse
5. utilizarea de site-uri web la care contribuie angajații nemulțumiți
6. efectuarea de descărcări mari și copierea fișierelor
7. accesul la rețea în afara orelor.

Tehnici de intruziune



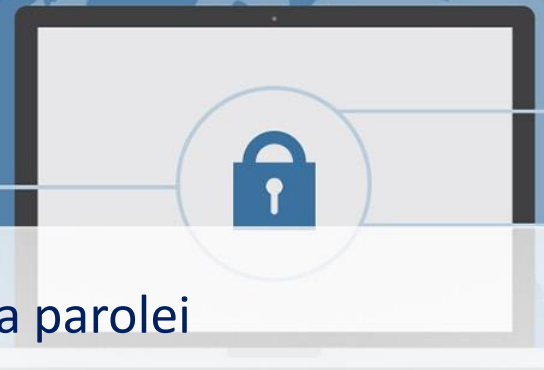
- Se urmărește obținea accesului și/sau creștere privilegiilor pe un sistem
- se folosesc adesea vulnerabilități de sistem/software
- obiectivul principal este de a dobândi parole
  - apoi exercitarea drepturilor de acces ale proprietarului
- Metodologia de atac de bază
  - identificarea țintei și colectarea informațiilor
  - accesul inițial
  - escaladarea privilegiilor
  - acoperirea/ștergerea urmelor

Aflarea parolei



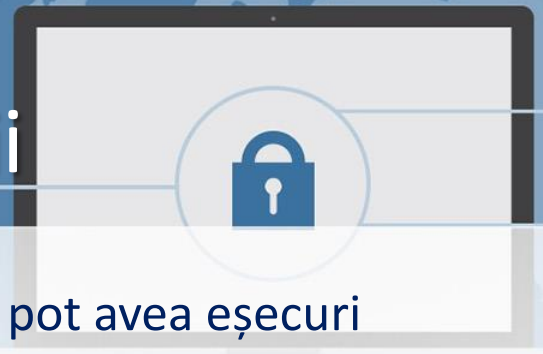
- unul dintre cele mai frecvente atacuri
- atacatorul știe un login (de la e-mail/pagina de web etc.)
- apoi încearcă să ghicească parola pentru resursa respectivă
  - parole implicite, parole scurte, căutări de cuvinte comune
  - informații despre utilizator (variații pe nume, ziua de naștere, telefon, cuvinte comune/interese)
  - caută în mod exhaustiv toate parolele posibile
- verificare prin *login* sau folosind un fișier de parole furat
- succesul depinde de parola aleasă de utilizator
- studiile arată că mulți utilizatori aleg parole slabe

Captură parolă



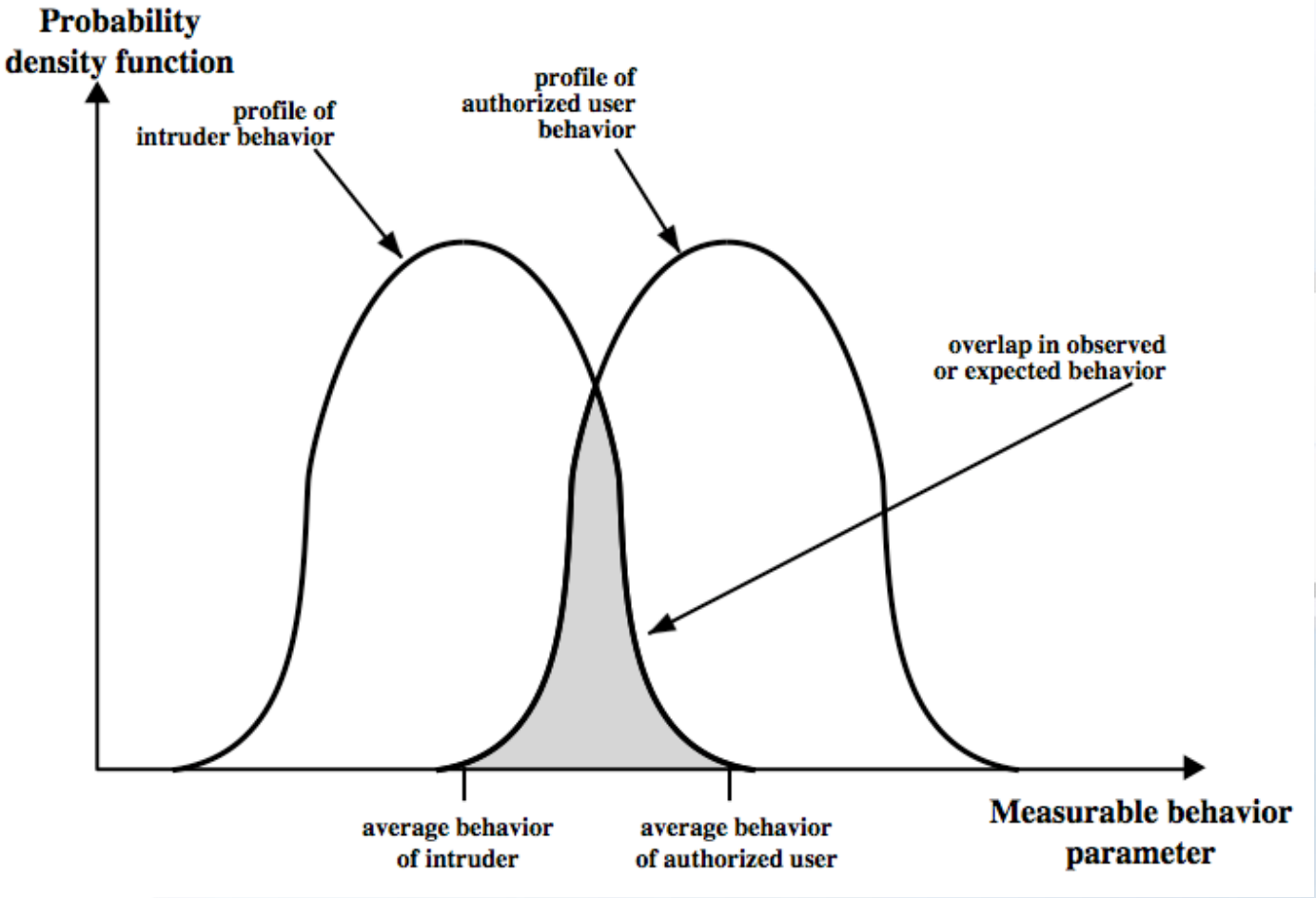
- un alt tip de atac implică captarea parolei
  - vizionarea peste umăr a parolei introduse
  - folosind un program cal troian pentru a colecta parole
  - monitorizarea unei conectări nesigure la rețea (Telnet, FTP, e-mail)
  - extragerea de informații înregistrate după login cu succes (istoric/cache web, ultimul număr format etc.)
- folosind date *login* valide se poate impersonaliza un utilizator
- utilizatorii trebuie să fie instruiți pentru a utiliza precauții adecvate și pentru a putea lua contramăsuri eficiente

Detectarea intruziunii

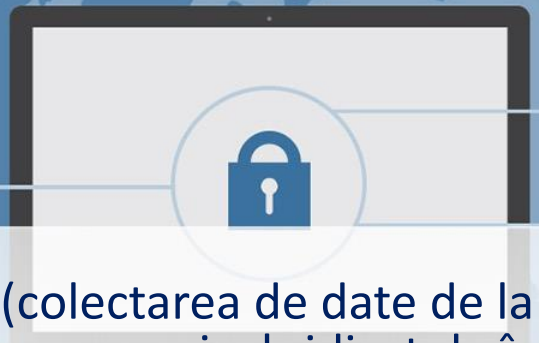


- Sistemele de securitate, inevitabil, pot avea eșecuri
- astfel e nevoie, de asemenea, de detecția intruziunilor, astfel încât să se poată:
  - bloca accesul dacă sunt detectate rapid
  - acționa ca măsură descurajatoare a atacurilor
  - colecta informații pentru a îmbunătăți securitatea
- Se presupune că intrusul se va comporta diferit față de un utilizator legitim
- va prezenta un element distinctiv pentru identificare

Detectarea intruziunii

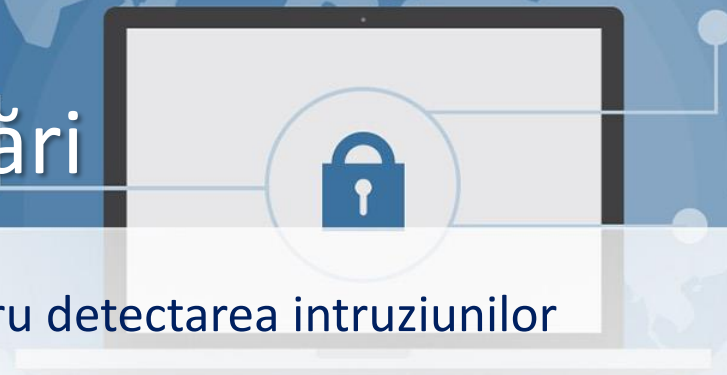


Abordări pentru detectarea intruziunii



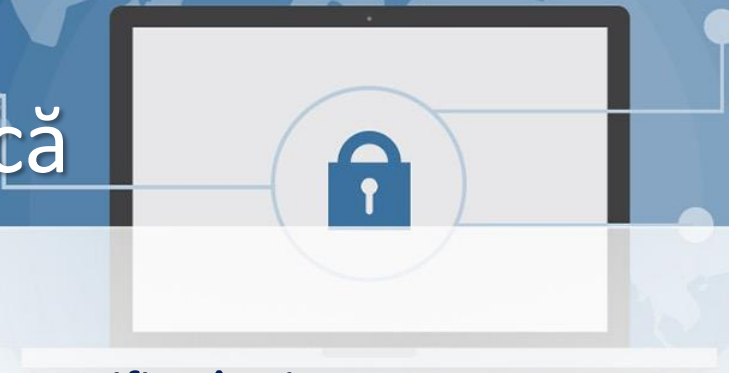
- Detectarea statistica a anomaliilor (colectarea de date de la utilizatori legitimi, utilizarea de teste statistice cu un nivel ridicat de încredere pentru a vedea dacă un nou comportament este legitim sau nu)
  - încercarea definirii comportamentului normal/așteptat
  - stabilirea pragul pentru frecvența apariției evenimentelor
  - bazat pe profil, detecția schimbării comportamentului
- Detectare bazată pe reguli
  - încercarea definirii unui set de reguli (comportament corect) pentru a putea decide dacă un comportament este sau nu o intruziune
  - Anomalie - deviere de la un model utilizat anterior
  - identificarea penetrări, sisteme expert caută comportamente suspecte

Verificare înregistrări



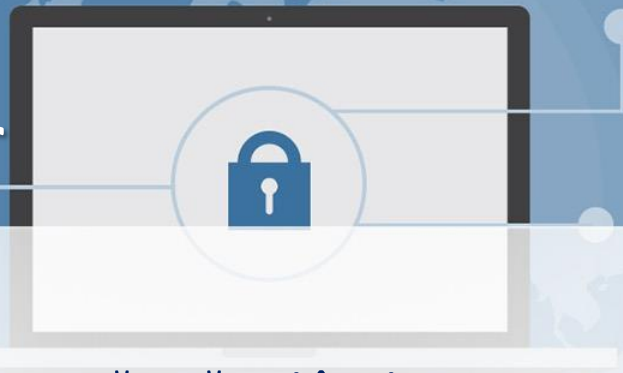
- Instrument fundamental pentru detectarea intruziunilor
- Înregistrări originale din sistem
  - parte din toate sistemele de operare multiutilizator comune
  - avantaj: sunt deja prezente și disponibile pentru utilizare
  - dezavantaj: poate să nu aibă informațiile dorite sau în forma dorită
- Înregistrări specifice detectării intruziunilor
  - create special pentru a colecta informații dorite
  - cost privind utilizarea de resurse suplimentare din sistem

Detectarea statistică



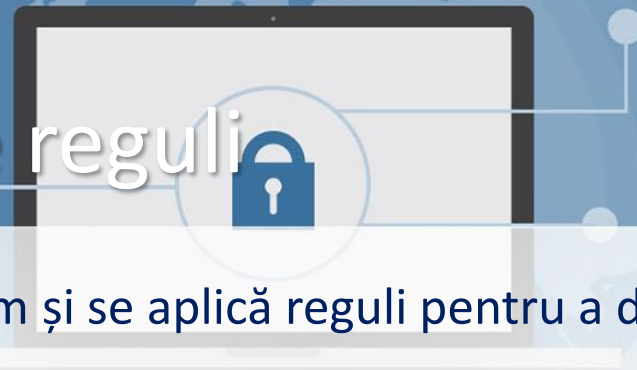
- Detectarea pragurilor
  - numărarea evenimentelor specifice în timp
  - dacă depășesc valoarea rezonabilă presupune intruziune
  - utilizat singur, mecanismul este un detector brut și ineficient
- Bazată pe profil
  - caracterizează comportamentul trecut al utilizatorilor
  - pentru a detecta apoi abateri semnificative de la profil
  - profilul constă dintr-o serie de mai mulți parametri
  - abordarea se bazează pe analiza înregistrărilor de sistem

Analiza înregistrărilor



- Baza abordărilor statistice
- analiza înregistrărilor pentru a obține măsurători în timp
  - Contor, ecartament, cronometru interval, utilizare resursă
- utilizează diverse teste pentru a determina dacă un comportament curent este acceptabil
  - deviație standard/medie, procese Markov, serii de timp,
  - Avantaj: nu este necesară o cunoaștere prealabilă a deficiențelor de securitate, astfel încât devine portabilă pe o varietate de sistem

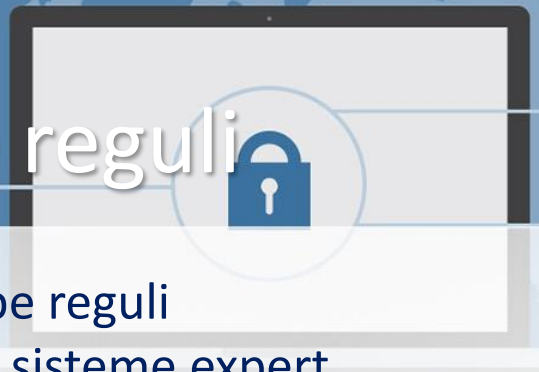
Detectare pe bază pe reguli



- Se observă evenimentele din sistem și se aplică reguli pentru a decide dacă activitatea este suspectă sau nu

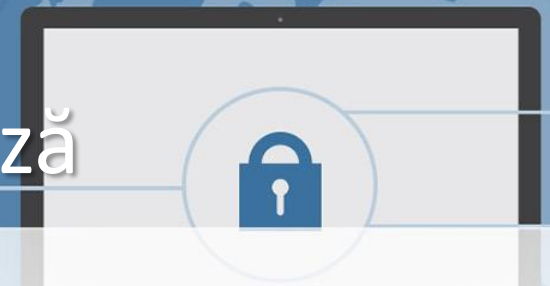
- Detectarea anomaliilor bazată pe reguli:
  - analiza înregistrărilor istoric de sistem pentru identificarea modelelor de utilizare și auto-generarea regulilor
  - apoi observarea comportamentul curent și verificarea împotriva regulilor pentru a vedea dacă este conform
  - ca și detectarea statistică a anomaliilor, nu necesită cunoștințe prealabile privind vulnerabilitățile de securitate ale sistemului

Detectare pe bază pe reguli



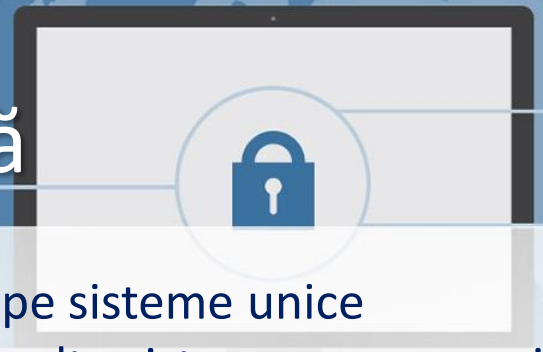
- identificarea de penetrare bazată pe reguli
  - utilizează tehnologia bazată pe sisteme expert
  - folosește reguli de identificare a atacurilor de penetrare cunoscute, sau atacuri care a exploata vulnerabilități cunoscute sau a comportamentului suspect
  - compararea înregistrărilor sau a stărilor sistem împotriva regulilor
  - regulile sunt specifice unor echipamente sau sisteme de operare
  - regulile sunt generate de experți care consultă și codifică cunoștințe specifice administratorilor și analiștilor de securitate
  - calitatea sistemului depinde de cât de bine se face acest lucru și de abilitățile celor care sunt implicați în definirea regulilor

Rata de eroare de bază



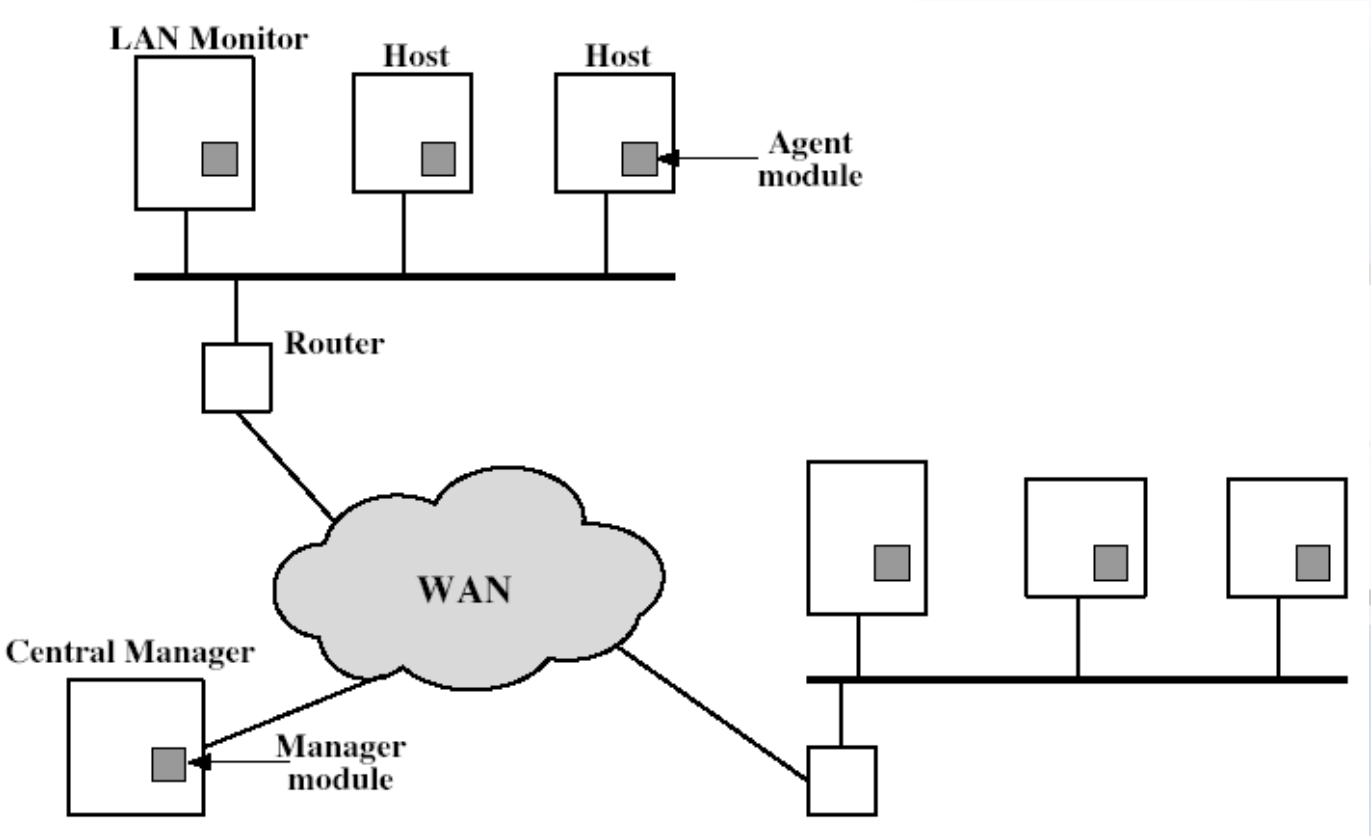
- practic un sistem de detectare a intruziunii trebuie să detecteze un procent substanțial de intruziuni, generând puține alarme false
- dacă sunt prea puține intruziuni detectate -> falsă securitate
- dacă sunt prea multe alarme false -> alarmele vor trebui ignorate, pierdere de timp
- Acest lucru (rată mare de detecție cu rată redusă de erori) este foarte greu de realizat
- Studiile arată că sistemele existente par să fie foarte performante din perspectiva ratelor de erori

Detectarea distribuită

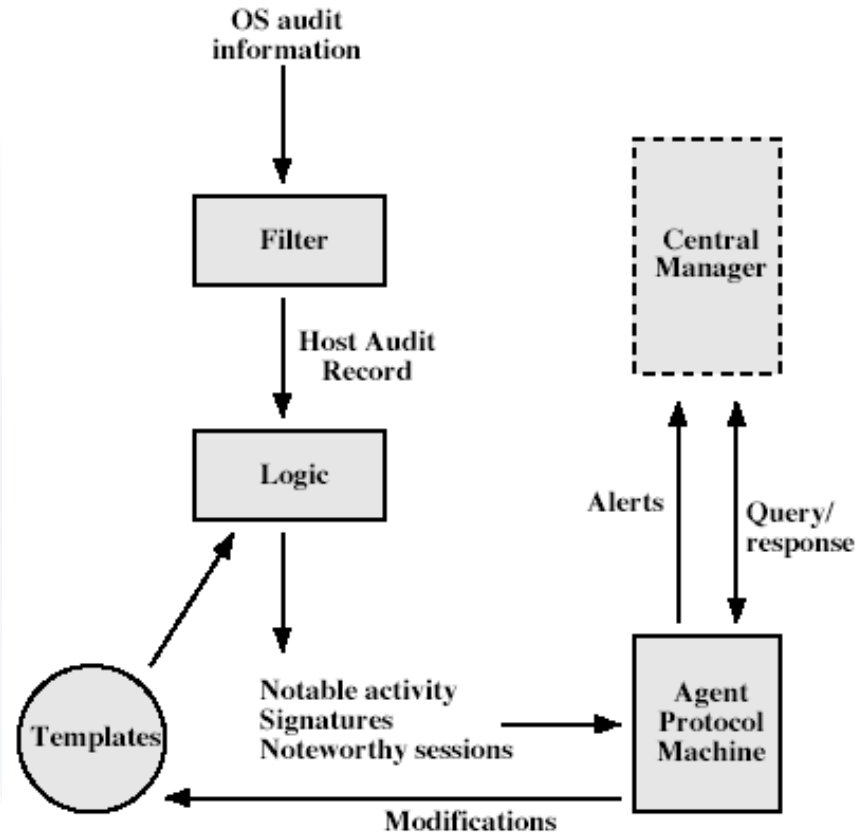


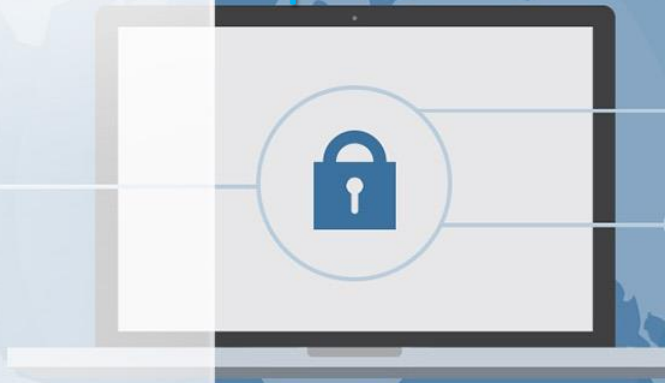
- Abordarea tradițională se bazează pe sisteme unice
- Dar organizațiile au de obicei mai multe sisteme care necesită și oferă servicii de securitate în rețea
- O abordare de apărare mai eficientă propune cooperarea și coordonarea acestor resurse împreună, pentru a detecta intruziuni
- Probleme ale IDS distribuite:
  - Gestiunea diferitelor formate de înregistrări
  - Integritatea și confidențialitatea datelor în rețea (transfer date)
  - Alegere arhitectura centralizată (un singur punct, simplitate dar poate exista aglomerări de procesare sau transfer de date) sau descentralizată (coordonarea mai multor centre de prelucrare)

Detectarea distribuită-arhitectură



Distributed Detection – Agent Implementation

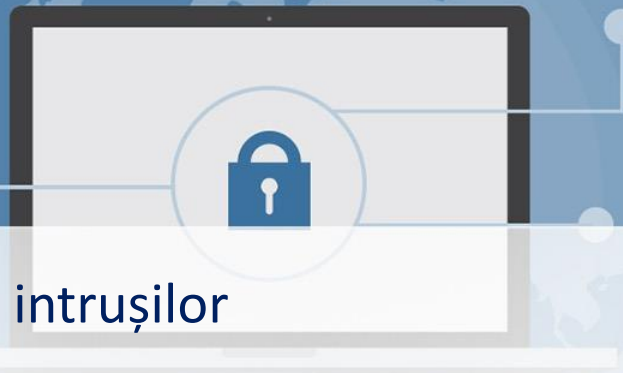




Honeypots

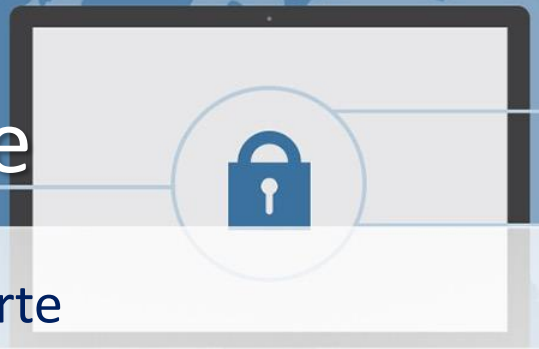
- sisteme de tip „momeală” pentru a atrage atacatori
  - separate de accesarea sistemelor critice
  - să colecteze informații cu privire la atacuri
  - pentru a încuraja atacatorul să rămână pe sistem, astfel încât administratorul să poată răspunde
- conțin informații fabricate/fictiv, aparent vulnerabile, la care un utilizator obișnuit nu ar avea acces, deci accesul devine suspect
- construite cu elemente de monitorizare și înregistrare a evenimentelor pentru a colecta informații detaliate privind activitățile atacatorilor
- pot fi sisteme de rețea unice sau multiple, distribuite
- grup de lucru IETF definește standardele necesare de detectare a intruziunilor pentru interoperabilitatea cu sisteme IDS, având diferite sisteme operare

Gestionarea parolei



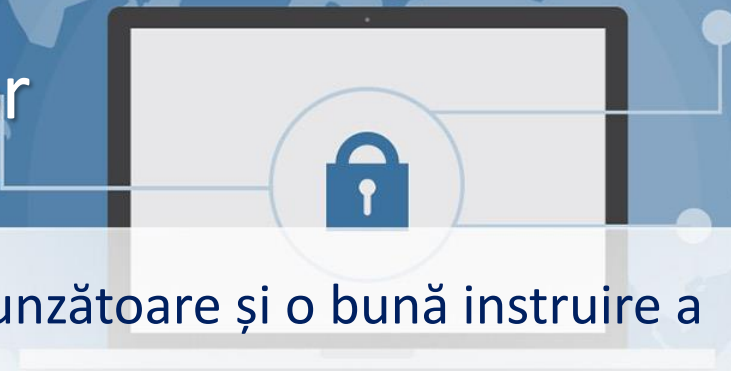
- Prima line de apărare împotriva intrușilor
- Utilizatorii furnizează atât:
  - Numele de cont/ID - stabilește privilegiile acelui utilizator
  - parolă – pentru a se identifica
- Parolele sunt stocate cel mai adesea criptate
  - Unix utiliza mecanismul DES multiplu (varianta cu salt)
  - sistemele mai recente utilizează funcții criptografice de tip hash (MD5)
- Ar trebui să fie bine protejat fișierul de parole pe sistem (controlul accesului)

Studii privind parolele



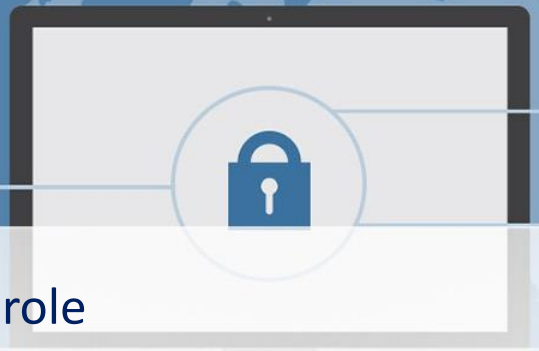
- Purdue 1992 - multe parole scurte
  - schimbarea parolelor pe 54 de mașini, de către 7000 de utilizatori, 3% foloseau 3 caractere sau mai puțin
- Klein 1990 - multe parole ușor de intuit
  - colecție de fișiere de parol, aproape 14000 de parole, un sfert din parole erau ușor de ghicit
- Concluzia este că utilizatorii aleg prea des parole slabe
- Este nevoie de o abordare pentru a contracara această problema
  - Forțarea utilizatorilor să nu poată să aleagă parole simple

Gestionarea parolelor - instruirea



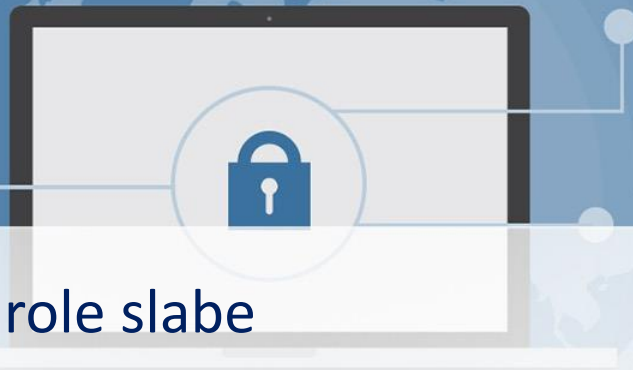
- Se pot folosi politici corespunzătoare și o bună instruire a utilizatorilor
- Instruirea privind importanța unei parole bune
- Linii directoare pentru parole bune
  - lungimea minimă (> 6)
  - nevoie de un amestec de litere majuscule și minuscule, numere, semne de punctuație
  - Nu sunt permise cuvinte din dicționar
- Dacă e posibil, recomandările tind să fie fi ignorate de către cei mai mulți utilizatori

Gestionarea parole
-parole generate



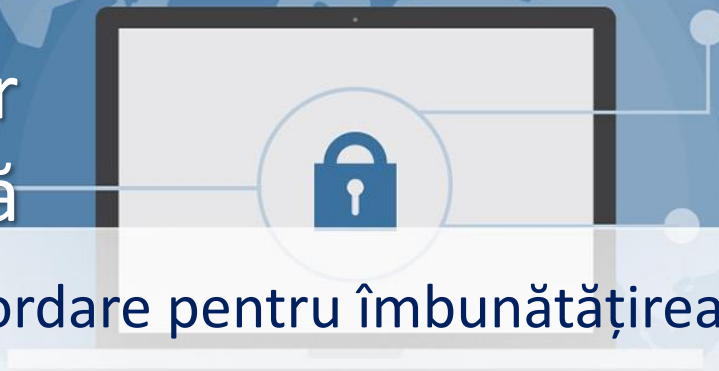
- Permite calculatorului să creeze parole
- Dacă sunt generate aleatoriu, probabil, nu ușor memorabile, ajung să fie notate (problemă)
- chiar cele care pot fi pronunțate sunt uitate
- mecanism greu acceptat de către utilizator
- FIPS PUB 181
  - este unul dintre cele mai bune generatoare de parole
  - are disponibilă atât descrierea cât și codul
  - generează cuvinte prin concatenarea de silabe aleatorii, pronunțabile

Gestionarea parolelor -verificarea reactivă



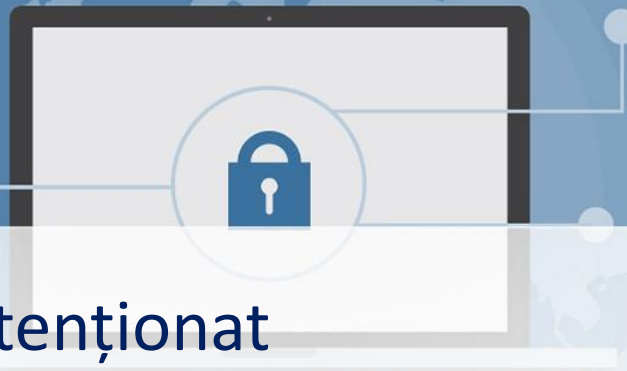
- Instrumente de identificat parole slabe
- Folosite periodic la nivelul sistemelor
  - există dicționare bune pentru aproape orice limbă/grup de interes
- Parolele sparte sunt dezactivate
- Dezavantaje:
  - Necesită consum intens de resurse
  - Parolele rele sunt vulnerabile până când sunt găsite

Gestionarea parolelor -verificarea pro-activă



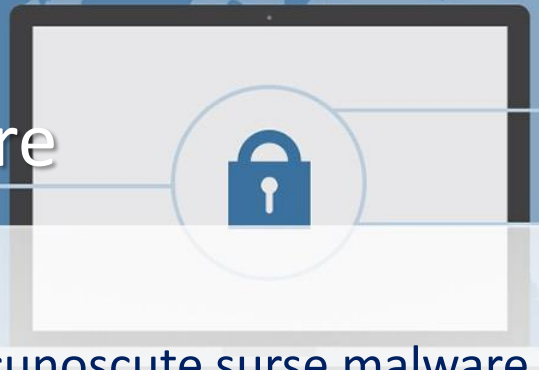
- Cea mai promițătoare abordare pentru îmbunătățirea securității parolei
- permite utilizatorilor să selecteze propria parolă
- Dar sistem verifica dacă parola este acceptabilă
  - aplicare simplă a regulilor
  - compara cu dicționarul de parole slabe
  - utilizarea mecanisme algoritmice (model Markov) pentru a detecta alegeri slabe
  - fără a genera sau utiliza dicționare vaste

Software rău intenționat



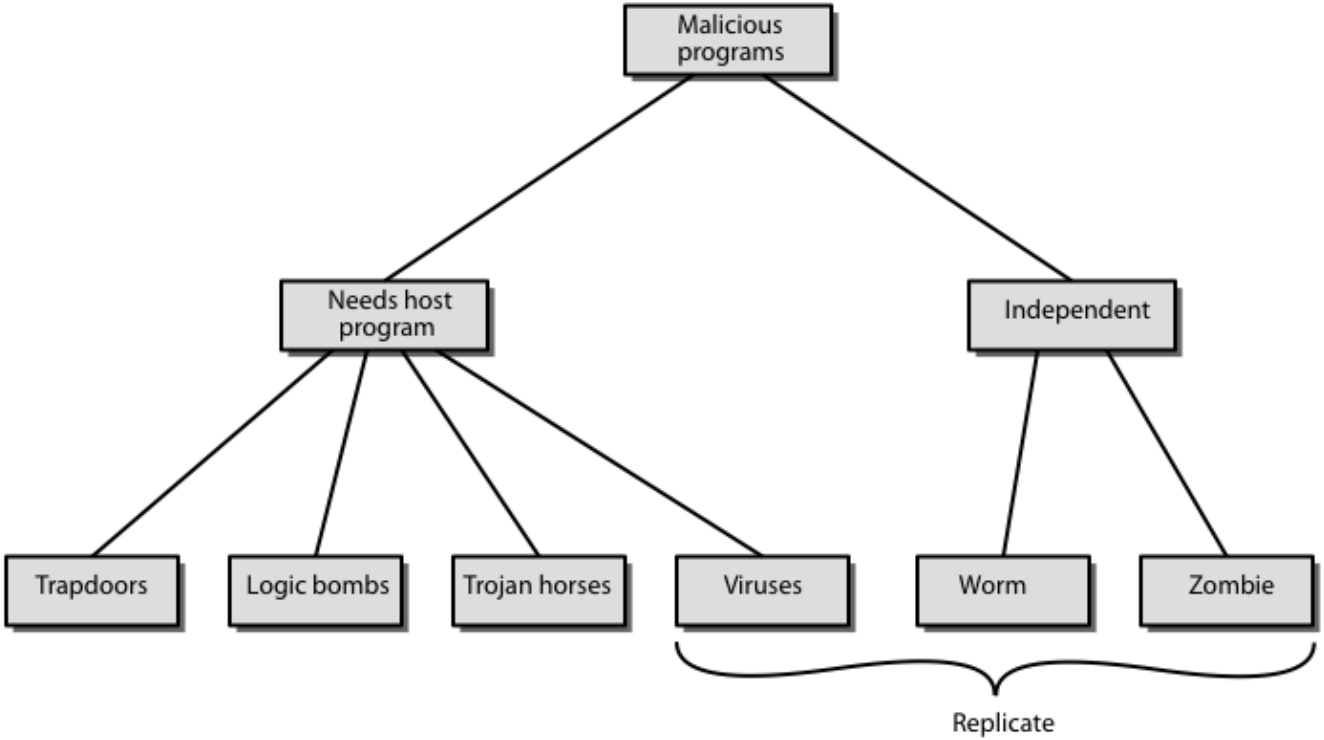
- Tipuri de software rău intenționat
- Viruşi
- Contramăsuri pentru viruși
- Viermi
- Atacuri Denial of Service distribuite

Viruși și alte surse malware

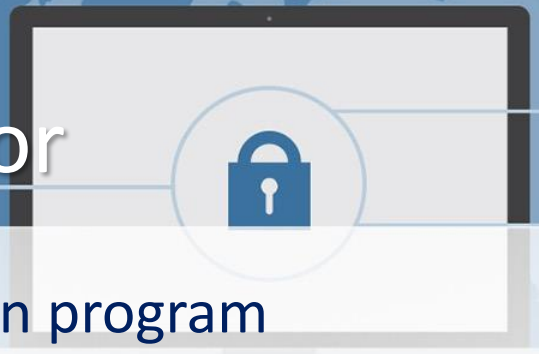


- Malware – Malicious software
- virușii de calculator sunt cele mai cunoscute surse malware
- e doar o familie de software rău intenționat
- produc efecte de obicei evidente la nivelul unui sistem
- și-au găsit loc în diverse rapoarte, știri, scenarii, filme (adesea exagerate)
- au atras, în general, mai multă atenție decât merită
- sunt totuși o preocupare justificată
  - *„A laptop infected with 6 of the most dangerous computer viruses in history was sold at auction to an anonymous buyer for $1.345 million”*
  - *ILOVEYOU, MyDoom, SoBig, WannaCry, DarkTequila, BlackEnergy*

Malware

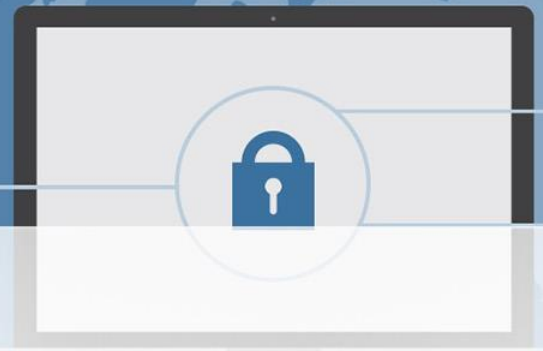

Malicious programs
Needs host program
Independent
Trapdoors
Logic bombs
Trojan horses
Viruses
Worm
Zombie
Replicate

Backdoor sau trapdoor



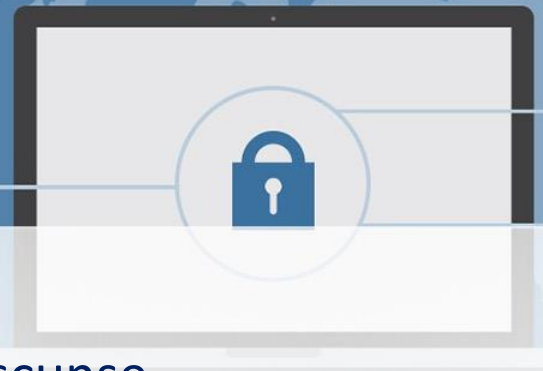
- Punct de intrare secret într-un program
- permite celor care cunosc accesul ocolind procedurile uzuale de securitate
- au fost frecvent utilizate de către dezvoltatori
- o amenințare atunci când pleacă în programe de producție care să permită exploatarea de atacatori
- foarte greu de blocat în sistemele de operare
- necesită o dezvoltare software corespunzătoare și actualizări

Logic Bomb



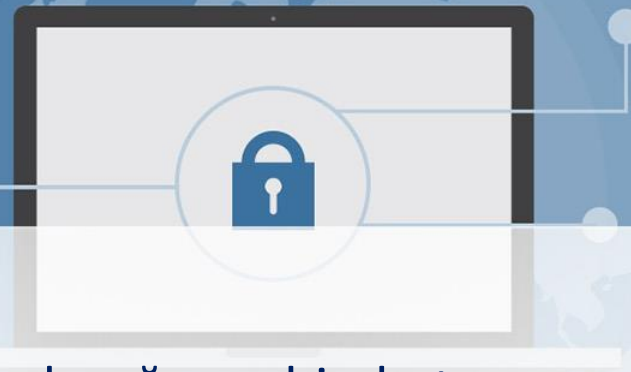
- Bomba logică
- Unul dintre cele mai vechi tipuri de software rău intenționat
- Cod încorporat într-un program legitim
- activat atunci când sunt îndeplinite condițiile specificate
  - de exemplu, prezența/absența unui fișier
  - anumită dată/oră
  - un anumit utilizator special
- Atunci când este declanșat de obicei sistemul este afectat
  - modifica/șterge fișiere/discuri, oprește sisteme etc

Trojan Horse



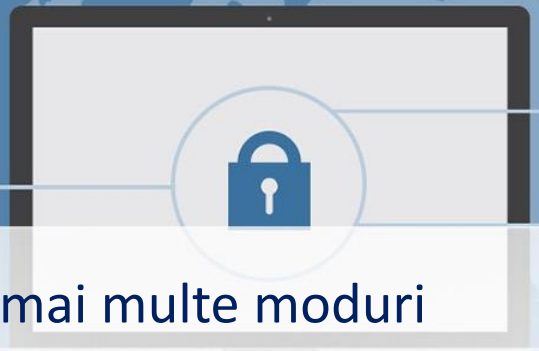
- Calul troian
- program cu efecte secundare ascunse
- care este, de obicei, aparent atractiv
  - de exemplu, un joc, un upgrade software etc.
- Atunci când rulează efectuează și unele activități suplimentare
  - permite atacatorului să obțină acces indirect (inițial accesul direct nu este permis)
- adesea folosit pentru a propaga un virus/vierme sau pentru a instala un backdoor
- sau pur și simplu pentru a distruge datele

Cod mobil



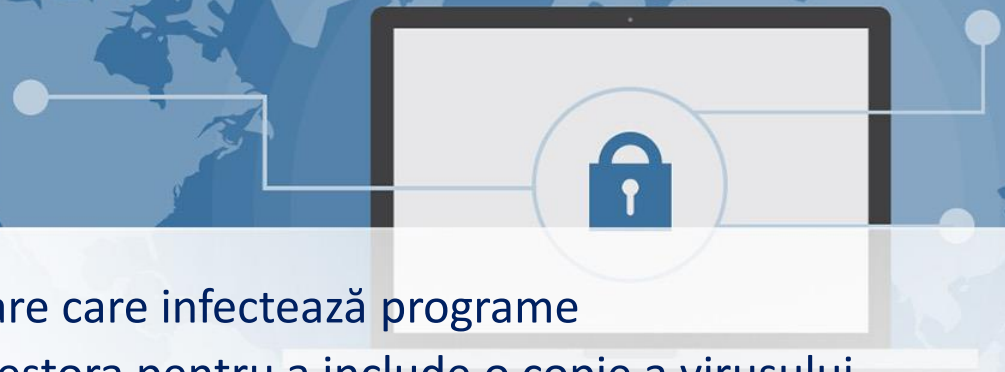
- Cod ușor portabil
- Un program/script/macro care rulează neschimbate
- pe diverse platforme eterogene
- sau in zone omogene larg răspândite (Windows)
- transmis de la sistemul de la distanță la sistemul local și apoi executat pe sistemul local
- de multe ori pentru a injecta un virus/vierme/cal troian
- sau pentru a efectua propriile atacuri
  - accesul neautorizat la date, compromisul rădăcină

Amenințări multiple



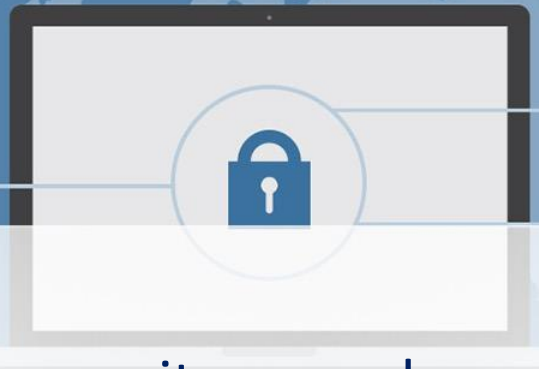
- Un malware poate funcționa în mai multe moduri
- viruși cu componente multiple infectează in mai multe moduri
  - Exemplu. mai multe tipuri de fișiere
- atacul combinat utilizează mai multe metode de infecție sau de transmitere
  - pentru a maximiza viteza de răspândire și severitatea atacului
  - pot include mai multe tipuri de malware
  - exemplu: Nimda conține vierme, virus, cod mobil
  - ar putea de asemenea folosi resursele de tip IM sau P2P

Viruşi



- O bucată de software care infectează programe
  - modificarea acestora pentru a include o copie a virusului
  - se execută în secret atunci când programul de gazdă este rulat
- Programe specifice sistemului de operare și echipamentului
  - Profitând de detaliile și slăbiciunile lor
- Un virus tipic trece prin faze diferite:
  - Așteptarea
  - Propagarea
  - Declanșarea
  - Executarea

Structura virusului



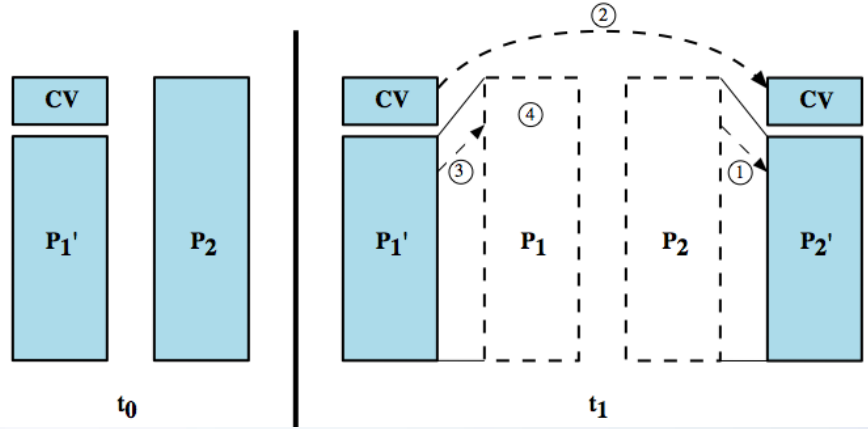
- Componente:
  - mecanismul de infectare - permite reproducerea
  - declanșator - eveniment care face sarcina utilă activă
  - sarcina utilă - acțiunea rău intenționată
- Poate fi rulat la începutul/sfârșitul/în timpul unui program
- De regulă când programul infectat este invocat, se execută codul de virus și mai apoi codul de program original
- Se poate bloca infecția inițială (mai dificil)
- sau propagarea virusului (mecanisme de control acces)

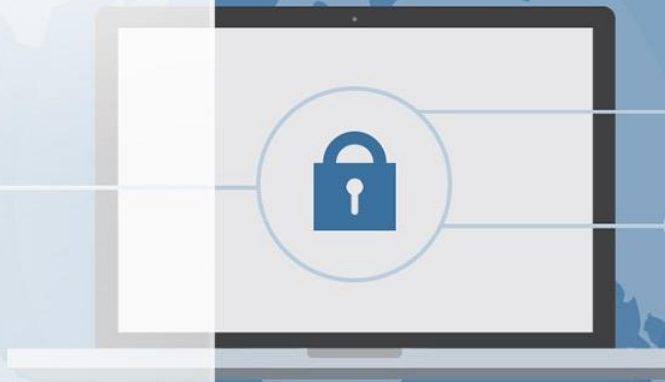
Structura virus

```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
          then goto loop
          else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine trigger-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

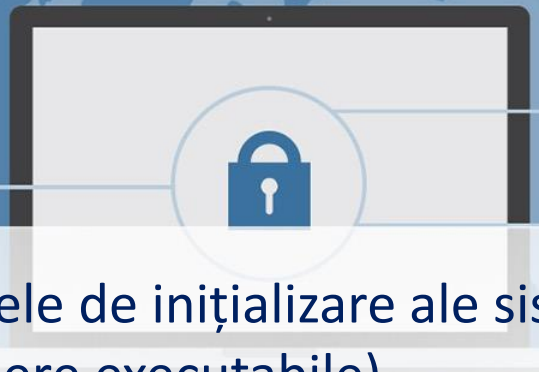
Compresie virus

```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
          {loop:
               file := get-random-executable-file;
          if (first-line-of-file = 01234567) then goto loop;
        (1)     compress file;
        (2)     prepend CV to file;
        }

main:   main-program :=
          {if ask-permission then infect-executable;
        (3)     uncompress rest-of-file;
        (4)     run uncompressed file;}
        }
```





Clasificare viruși

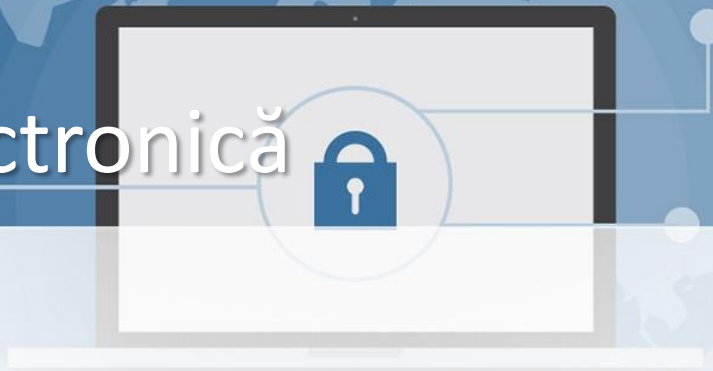


- sectorul de boot (afectează zonele de inițializare ale sistemului)
- infectează fișiere (infectează fișiere executabile)
- macro (componente interpretate de diferite aplicații)
- criptat (creează o cheie cu care se criptează restul virului, la execuție se decriptează codul folosind cheia, la replicare se generează o nouă cheie)
- ascuns (se ascunde pentru a nu fi detectat)
- polimorf (își modifică „semnătura” la fiecare execuție)
- metamorfic (își modifică atât comportamentul cât și forma)

Virus macro

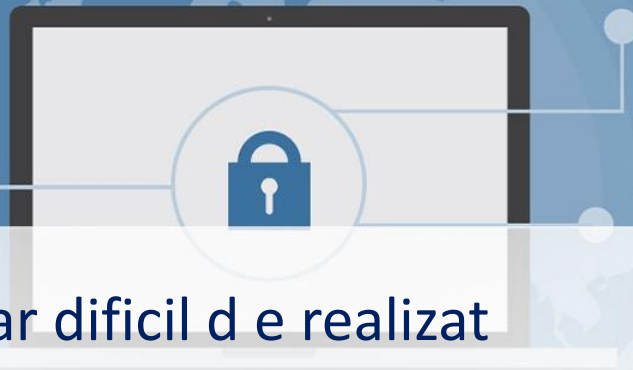
- a devenit foarte frecvent la jumătatea anilor 1990
  - independent de platformă
  - infectare documente
  - ușor de răspândit
- exploatează facilitățile macro ale aplicațiilor Office (Excel)
  - program executabil încorporat în documente Office
  - adesea o formă a limbajului Basic
- versiuni mai recente includ protecția lansării de macro (avertizare la lansare)
- recunoscute de multe programe anti-virus

Viruși de poștă electronică



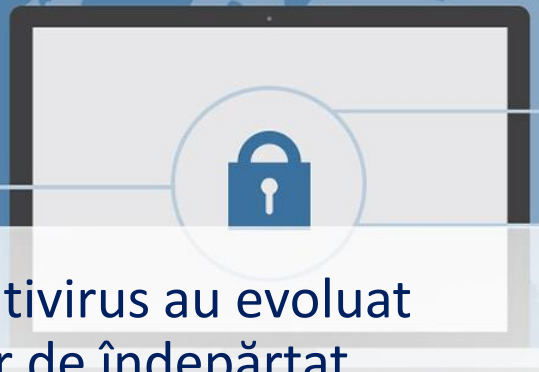
- Dezvoltare mai recentă
- de ex. Melissa
  - Exploatează funcțiile MS Word macro în documente atașate
  - dacă se deschide atașarea, componenta macro se activează
  - trimite e-mail tuturor utilizatorilor din lista de adrese
  - și provoacă daune locale
  -
- Versiuni declanșate la citirea unui e-mail
- prin urmare, propagare mult mai rapidă

Contramăsuri



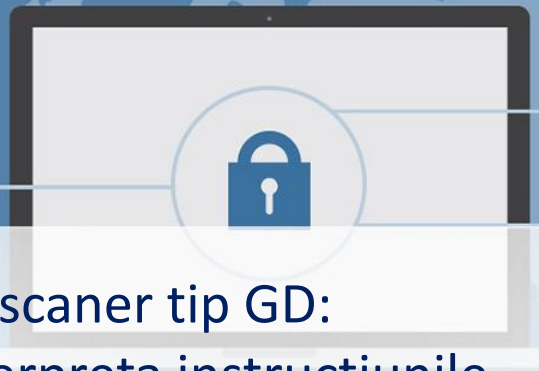
- Prevenirea - soluția ideală, dar dificil d e realizat
- Necesar:
  - Detectare
  - Identificare
  - Eliminare
- Dacă este detectat, dar nu poate fi identificat sau eliminat, atunci programul infectat trebuie șters sau înlocuit

Evoluție antiviruși



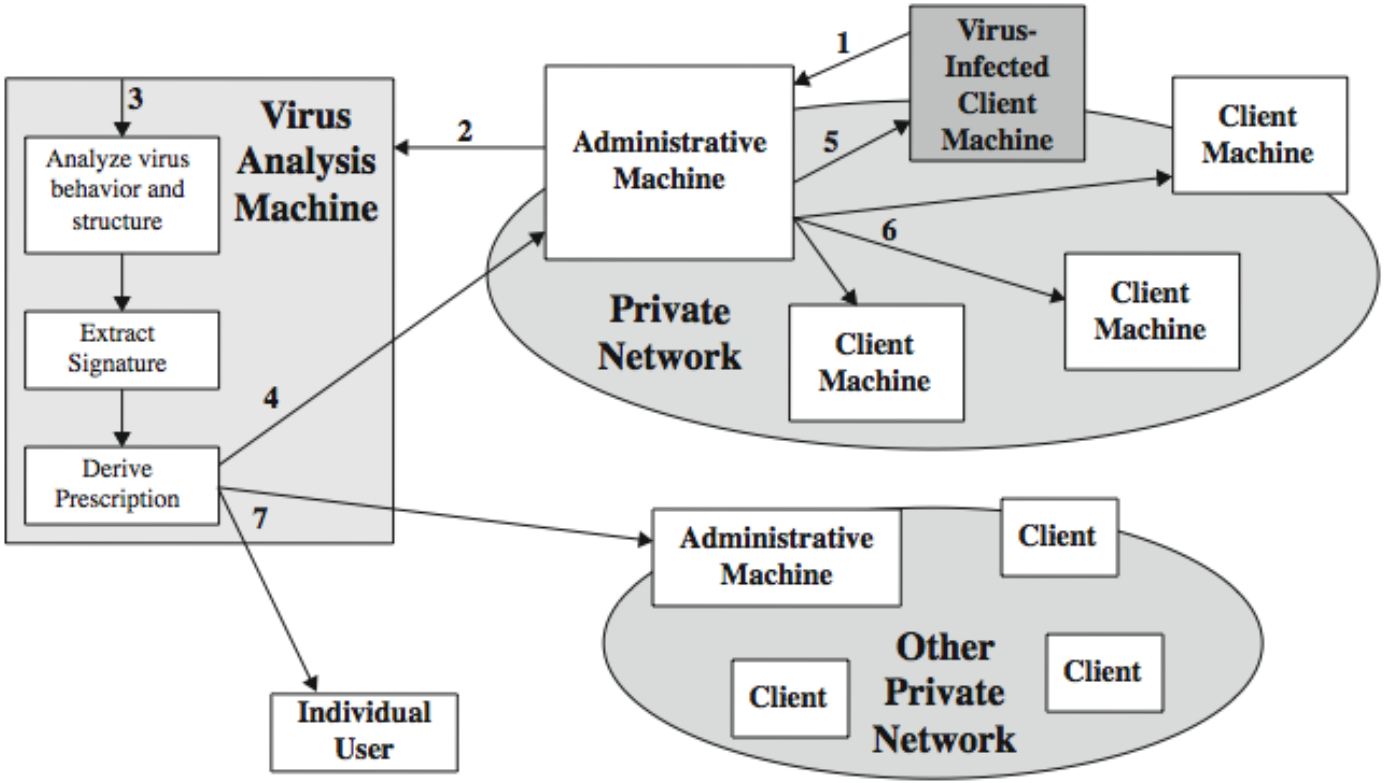
- Atât virușii cât și tehnologiile antivirus au evoluat
- viruși timpurii - cod simplu, ușor de îndepărtat
- devenind tot mai complecși, astfel încât trebuie contramăsuri
- Generații de aplicații antivirus
  1. Identificare semnătură specifică (doar viruși cunoscuți)
  2. Reguli euristice (descoperire fragmente de cod asociate cu viruși, verificarea integrității, sume de control, hash-uri)
  3. Identificarea acțiunilor (prin programe rezistente)
  4. Soluții combinare (în plus, pot avea componente de control al accesului pentru limitare atacurilor de penetrare a sistemelor, limitarea actualizării fișierelor în vederea propagării)

Decriptare generică



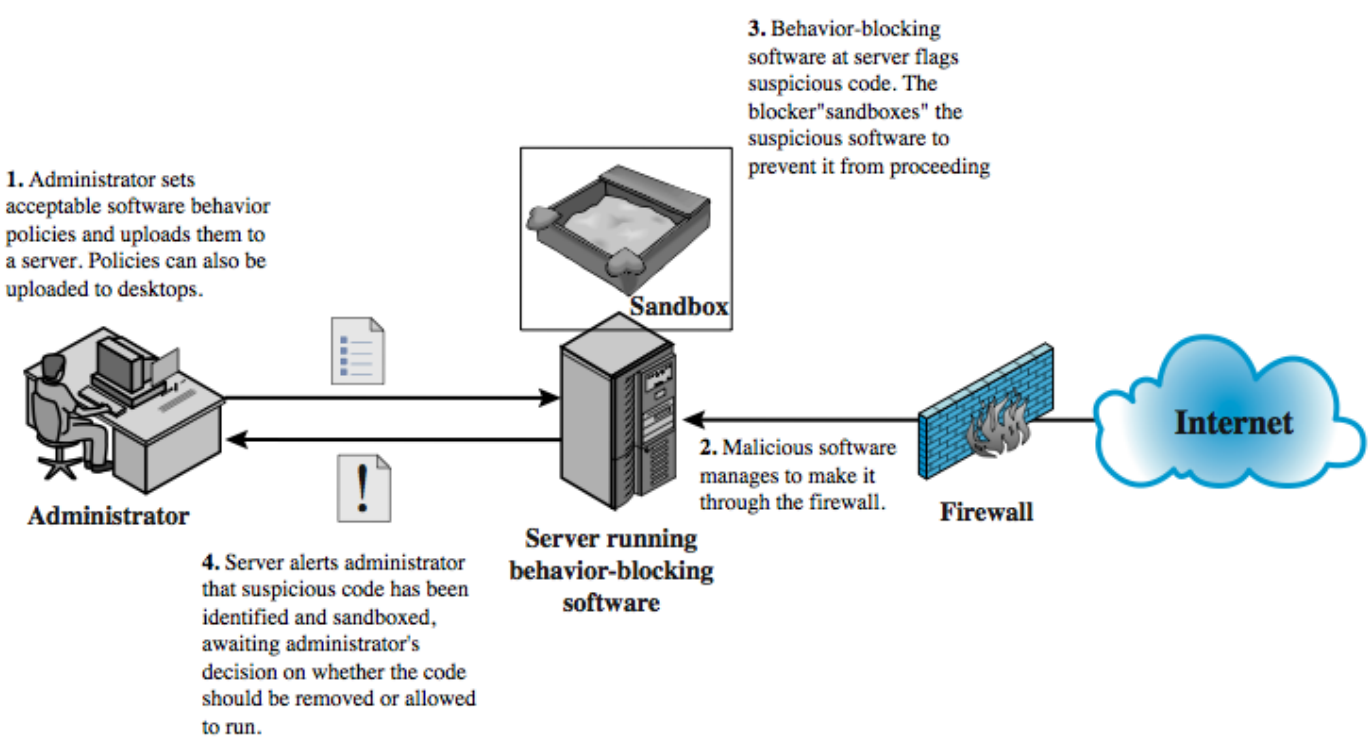
- Rulează fișiere executabile prin scaner tip GD:
  - emulator CPU - pentru a interpreta instrucțiunile
  - scanner virus - pentru a verifica semnături virus cunoscute
  - modul de control emulat - pentru a gestiona execuția procesului
- Permite virusului decriptarea în cadrul interpretorului
- Scanarea periodică a semnăturilor de virus
- problemă legată de timpul necesar pentru a interpreta și scana
  - compromis între detectare și întârzierea în timp

Sistem imunitar digital

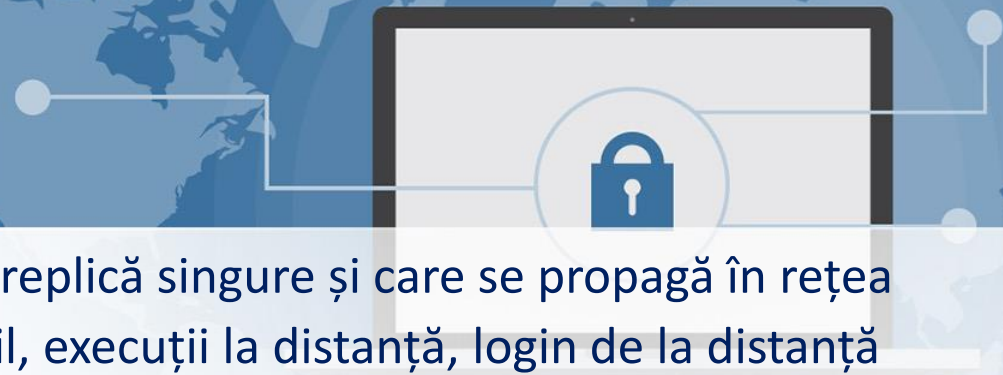


- Abordare IBM (Symantec)

Aplicații de blocare

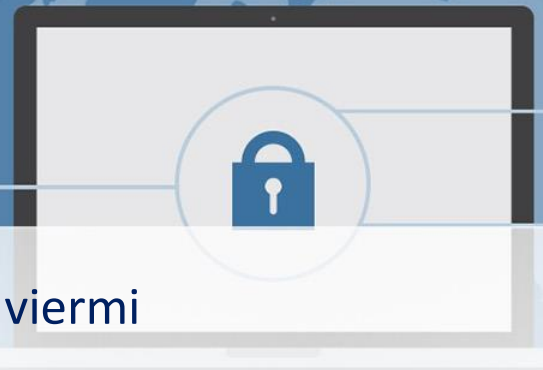


Viermi



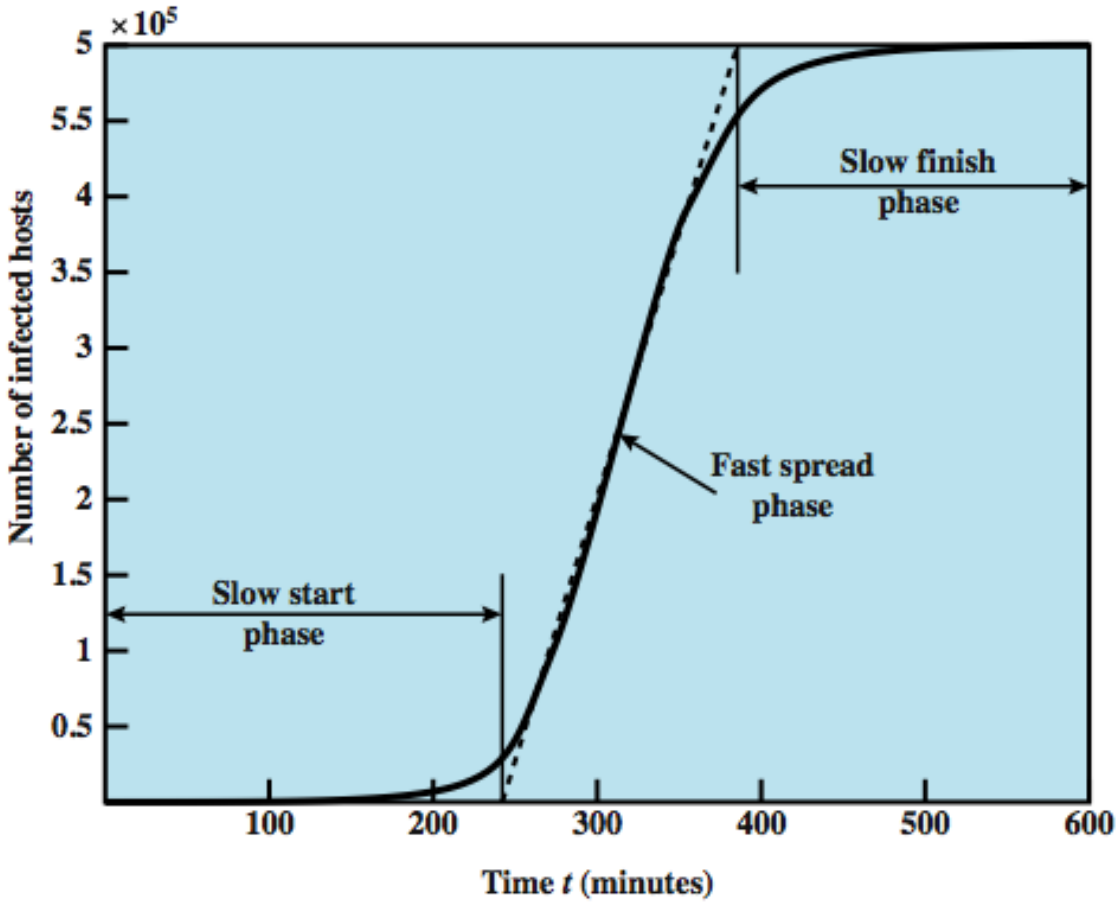
- Programe care se replică singure și care se propagă în rețea
  - folosind e-mail, execuții la distanță, login de la distanță
- Are faze, ca un virus:
  - Așteptare, propagare, declanșare, execuție
  - faza de propagare: căută alte sisteme, se conectează la ele, se copie singur și se execută
- se poate deghiza ca fiind un proces de sistem
- Conceptul introdus în nuvela SF a lui John Brunner, „Shockwave Rider”
- prima implementare realizată de laboratoarele Xerox Palo Alto în anii 1980
  - Nemalițioasă, căuta sisteme în așteptare pentru a rula procese intense

Viermele Morris



- Unul dintre cei mai bine cunoscuți viermi
- lansat de Robert Morris în 1988
- diferite atacuri asupra sistemelor UNIX
  - Spargerea fișierelor de parole pentru a face autentificare pe alt sistem
  - exploatarea unui bug în protocolul *finger* (vizualizare utilizatori la distanță)
  - exploatarea unui bug în *sendmail*
- Odată reușită rularea, se are acces de consolă la distanță
  - Se trimis program de inițializare pentru a copia viermele

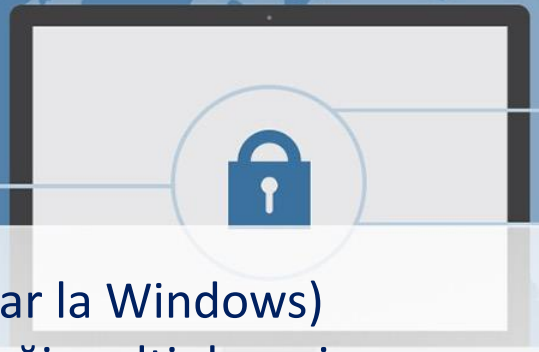
Model de propagare vierme



Atacuri vierme recente

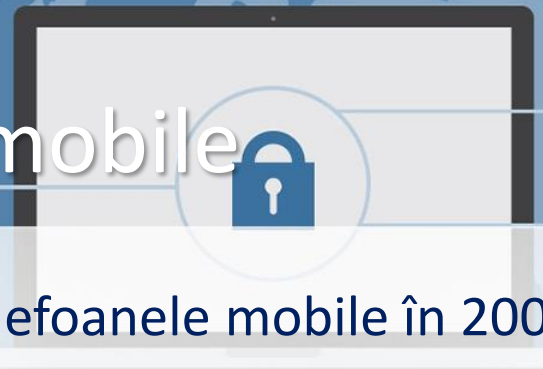
- Code Red
  - July 2001 exploatează un bug MS IIS, dezactivează verificarea fișierelor
  - testează adrese IP aleatorii, realizează atacuri DDoS, A afectat 360000 de servere in 14 ore
- Code Red II – include un backdoor
- SQL Slammer
  - early 2003, atacă serverul MS SQL, Compact și rapid
- Sobig.f
  - Exploatează servere open proxy, deschizând surse de spam
- Mydoom
  - Trimitere de email-uri în masă, a apărut în 2004
  - Instalare backdoor in sistemele infectate, replicare 1000ori/minut, 100 mil. mesaje in 36 ore
- Familia de viermi Warezov
  - Scanează fișiere pentru a identifica adrese e-mail, se trimite singur in attachment

Tehnologii specifice



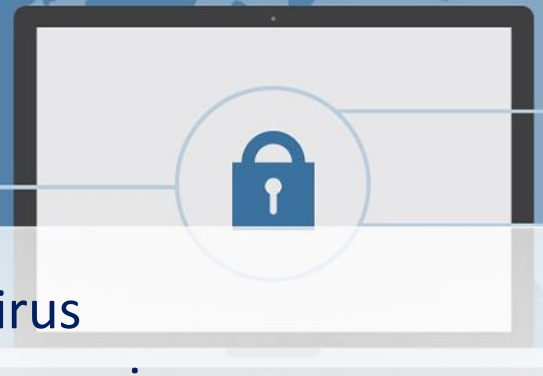
- Multiplatformă (nu se limitează doar la Windows)
- Exploatare multiplă (penetrare pe căi multiple, prin servere web, aplicații browser, email, partajare de fișiere etc.)
- răspândire ultrarapidă (identificarea prealabilă a adreselor sistemelor vulnerabile)
- Polimorfism (fiecare nouă copie are un cod nou generat din mers)
- Metamorfism (pe lângă o nouă formă, poate avea și un nou comportament)
- vehicule de transport (pentru instrumente de atac distribuit, DDoS)
- zero-day exploit (exploatează o vulnerabilitate necunoscută care este identificată după răspândirea viermelui)

Viermi de telefoane mobile



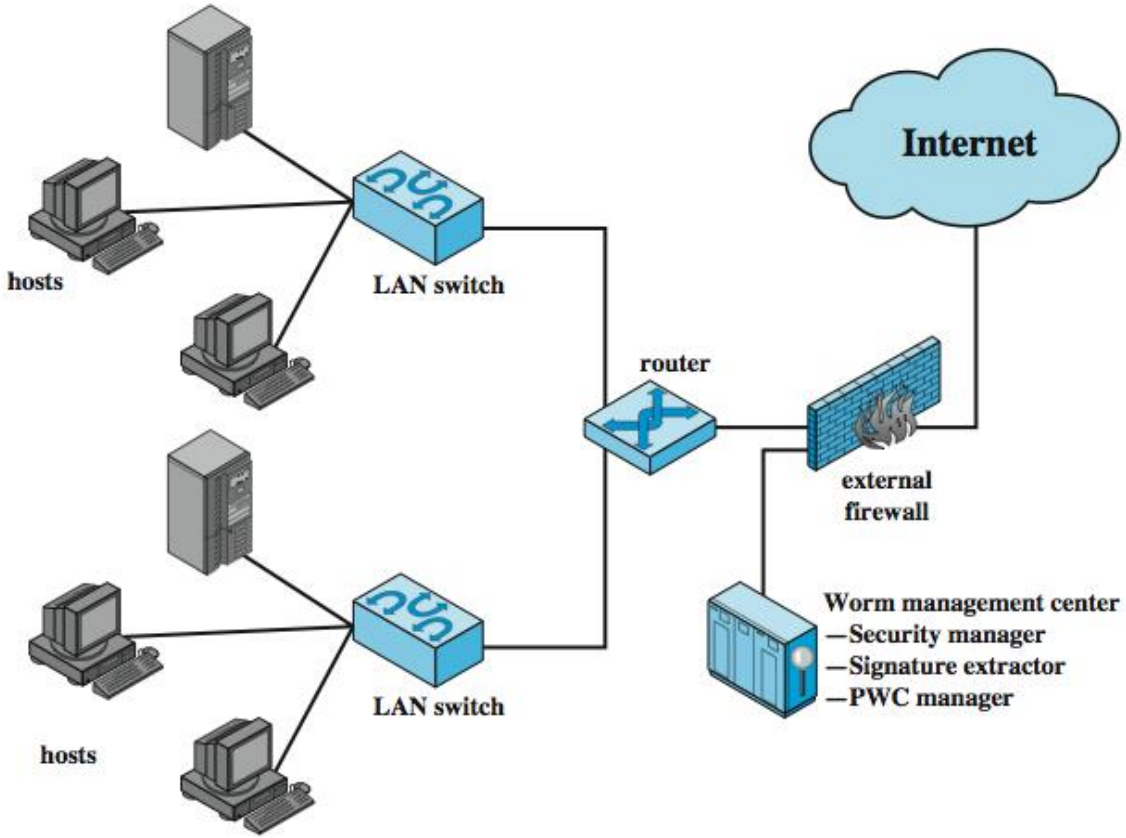
- apărut pentru prima dată pe telefoanele mobile în 2004
  - smartphone țintă care poate instala aplicații
- comunică prin Bluetooth sau MMS
- dezactivare telefon, șterge date de pe telefon sau trimite mesaje
- CommWarrior, lansat în 2005
  - Se reproduce folosind Bluetooth la telefoanele din apropiere
  - și prin MMS utilizând numere de agendă
  - Se copie pe card sau intre programele din telefon

Combaterea viermilor

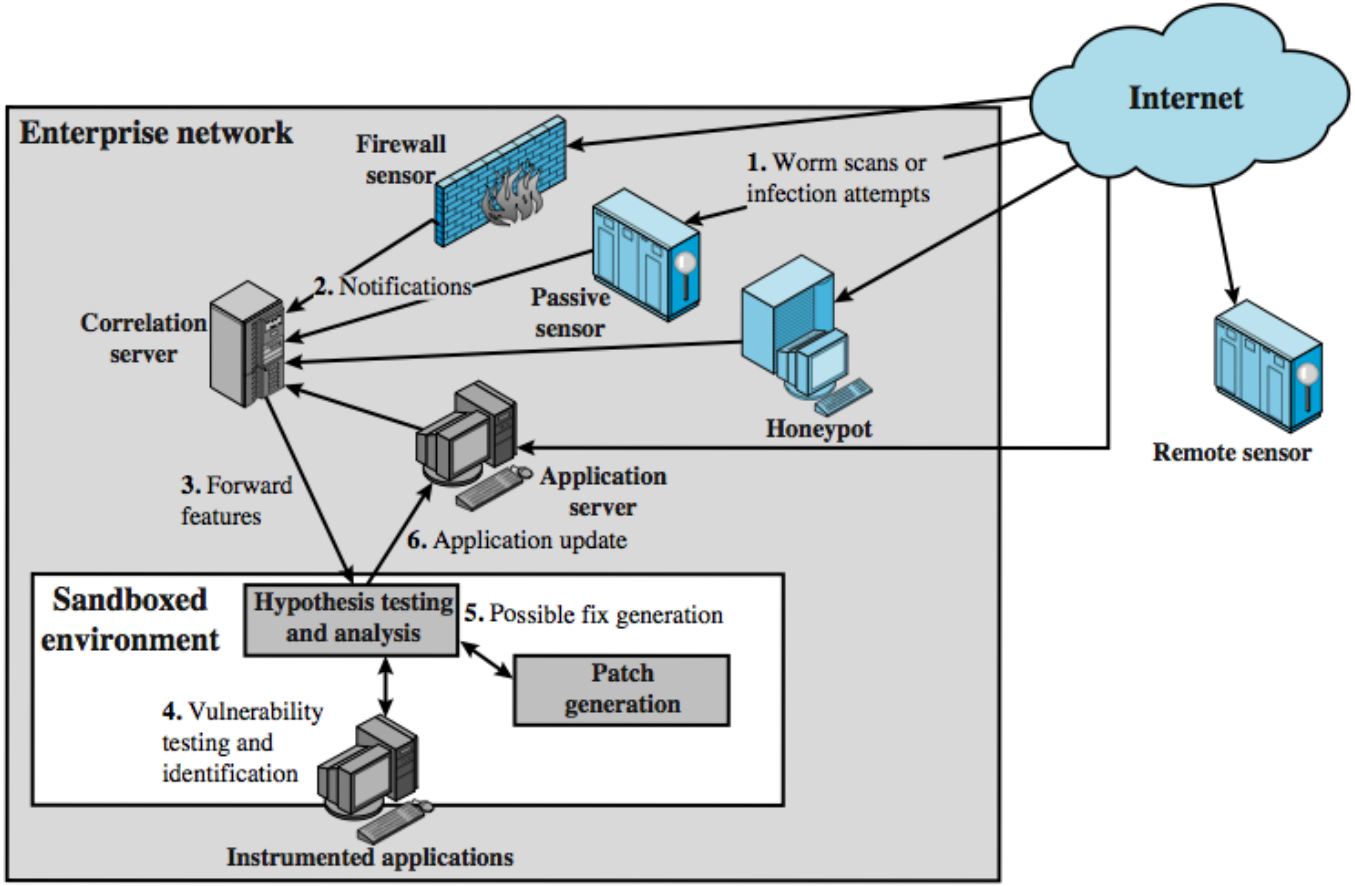


- Suprapunere cu tehnicile anti-virus
- sistemul antivirus poate detecta un vierme
- viermi provoca, de asemenea, activitate semnificativă în rețea
- Abordări de apărare includ:
  - filtrare pe bază de semnături specifice viermilor
  - sisteme de izolare a viermilor pe bază de semnături
  - sisteme de izolare a viermilor pe bază de conținut
  - lansarea de procese aleatorii de detectare a scanării
  - Limitarea ratei de transfer și blocarea traficului pentru un sistem identificat a fi compromis

Izolarea viermilor



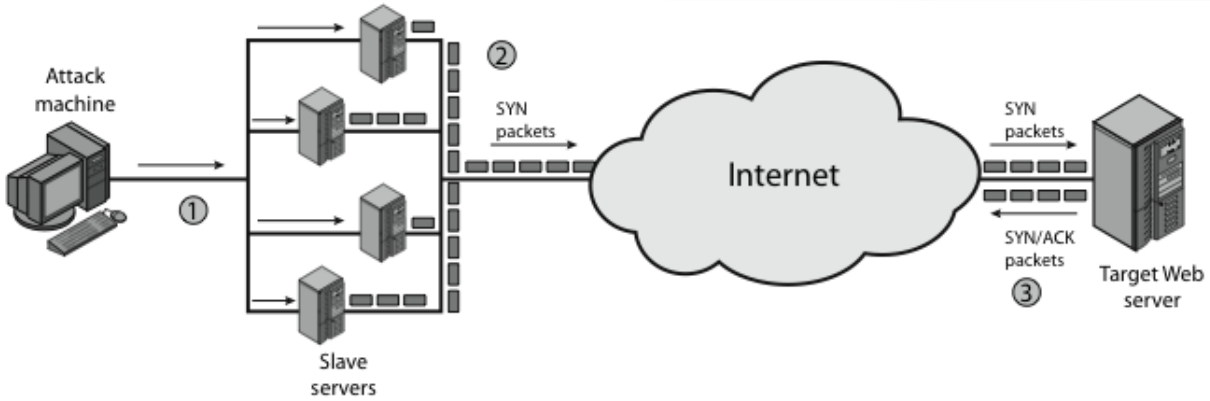
Protecția în rețea



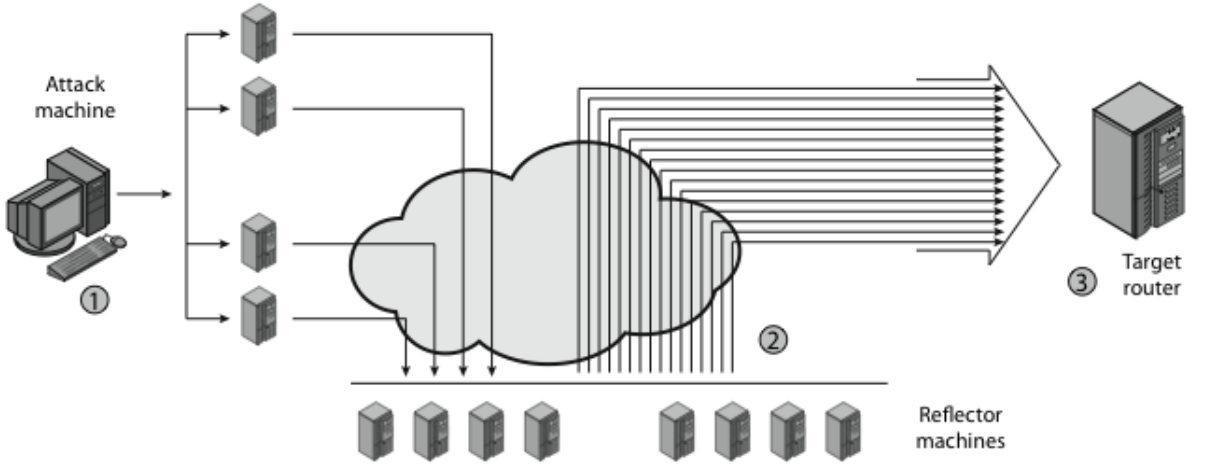
Atacuri Denial of Service distribuite (DDoS)

- Atacurile Denial of Service (DDoS) distribuite formează o amenințare de securitate semnificativă
- sistemele de rețea devin indisponibile
- fiind inundate cu trafic inutil
- folosind un număr mare de sisteme compromise ("zombi„)
- complexitate în creștere a atacurilor
- tehnologii de apărare se luptă pentru a face față
- fiind mult mai dificil de identificat și localizat atacatorul real

DDoS

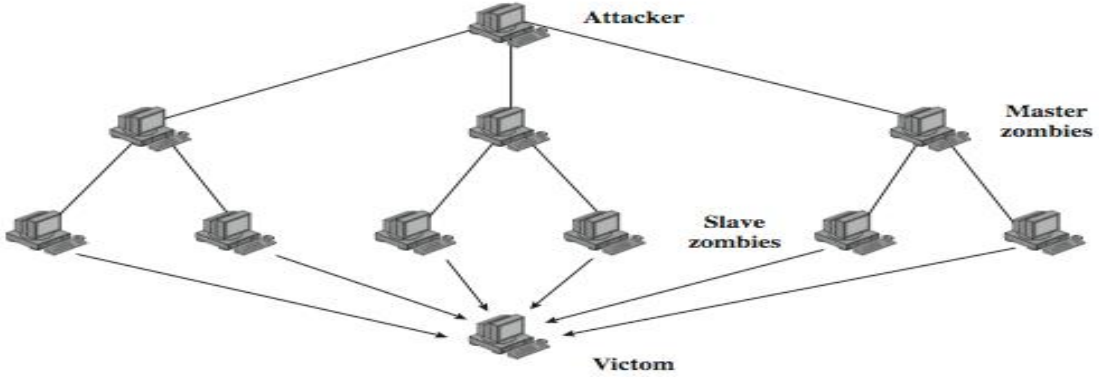


(a) Distributed SYN flood attack

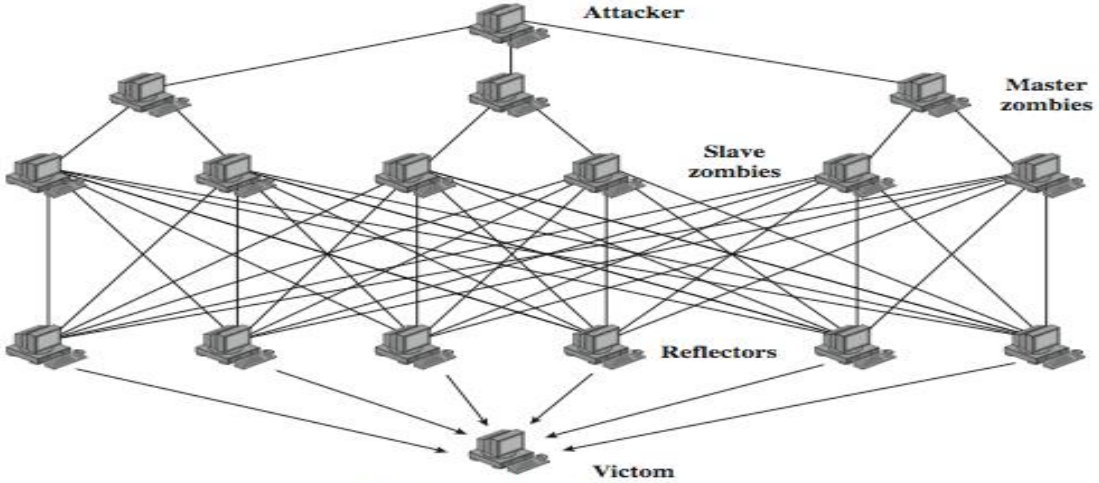


(a) Distributed ICMP attack

DDoS Tipuri



(a) Direct DDoS Attack

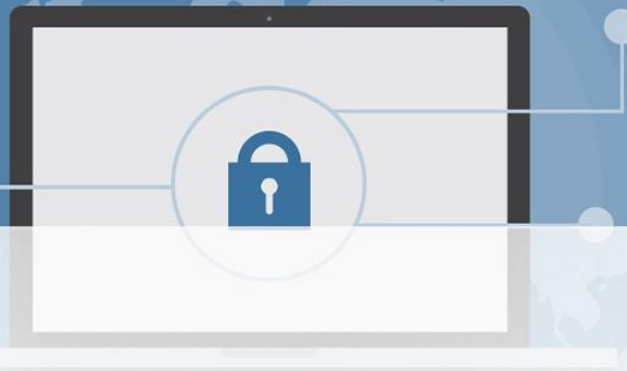


(b) Reflector DDoS Attack

Construirea unei rețele de atac

- Trebuie să infecteze un număr mare de zombi
- Necesar:
- software pentru a implementa atacul DDoS
- o vulnerabilitate neacoperită pe mai multe sisteme
- strategie de scanare pentru a găsi sisteme vulnerabile
  - aleatoriu,
  - Hit-list, (liste de stații vulnerabile)
  - Informații legate de topologia rețelei,
  - subrețea locală

Contramăsuri DDoS



- Linii mari de apărare:
  - Prevenire atac (înainte)
  - detectare și filtrare atacuri (în timpul)
  - identificare sursa de atac (după)
- gamă imensă de posibilități de atac
- prin urmare, e necesară și o evoluție a contramăsurilor