Protectia Sistemelor De Calcul Impotriva Atacurilor Informatice

ARGUMENT

In viața noastra de zi cu zi, calculatoarele sunt ceva obisnuit, ba chiar indinspensabil in unele cazuri. Se poate spune, pe drept cuvant ca traim intr-o societate informatizata. In zilele noastre, intalnim calculatoare peste tot. Toate acestea se datoreaza faptului ca ne dam seama din ce in ce mai mult ca PC-ul ne usureaza munca. Dar trebuie subliniat faptul ca un calculator este de fapt o 'mașinarie' care prelucreaza o serie de informații pe care i le dam. Societatea informațonala poate fi gasita la intersecția dintre ramurile ,alta data distincte, ale telecomunicațiilor si calculatoarelor, grupate in jurul informației digitale.

Informația, este elementul esențial din acest intreg lanț. Dezvoltarea rapida si complexa a societații a dus inevitabil la o sporire insemnata a volumului de informații care, inevitabil poate fi si ținta raufacatorilor. Deci, noi trebuie sa ne protejam informațiile si activitațile cu ajutorul unor anumite programe pe care eu le voi prezenta in accest proiect de atestat.

Fără un sistem de securitate implementat și funcțional, sistemele informatice, de telecomunicații și datele prelucrate, stocate sau trasportate de acestea pot fi oricând supuse unor atacuri informatice. Unele atacuri sunt pasive - informațiile sunt monitorizate sau copiate, iar alte atacuri sunt active - fluxul de informații este modificat cu intenţia de a corupe sau distruge datele sau chiar sistemul sau rețeaua în sine. Sistemele informatice și de telecomunicații, rețelele formate de acestea și informațiile pe care le dețin sunt vulnerabile la numeroase tipuri de atacuri dacă nu sunt apărate de un plan de securitate informatică eficient.

« Modul cum culegi, administrezi si folosesti informația fac din tine un castigator sau un infrant in viața »,
asa subliniaza Bill Gates rolul actual al sistemelor de calcul in viata noastra, a tuturor.

NOȚIUNI INTRODUCTIVE

Ca o definiție, sistemul de calcul reprezinta un ansamblu de componente hardware (dispozitive) si componente software (sistem de operare si programe specializate) ce ofera servicii utilizatorului pentru coordonarea si controlul executarii operațiilor prin intermediul programelor.

Principiile de baza ale securitații sistemelor informatice s-au schimbat relativ putin in ultimii ani. Exista doua mari categorii – protecția la nivel fizic (garduri, uși cu incuietori, lacate, etc.) si la nivel informțional (accesare prin intermediul unor dispozitive electronice si/sau a unor aplicații software, a informațiilor dintr-un sistem de clacul – in mod general, in mod particular, informațiilor dintr-un calculator dintr-o rețea de calculatoare).

Utilizarea echipamentelor de tip router si aplicarea listelor de control al accesului, impreuna cu controlul traficului ce intra si iese din rețele utilizand soluții firewall reprezinta si in prezent, tehnicile principale pentru protecție perimetrala. Facand parte din categoria tehnicilor de tip pasiv, cele doua nivele de protecție au fost continuu optimizate din punct de vedere al performanțelor, functionalitaților si al administrarii.

Creșterea susținuta a numarului de atacuri si a complexității acestora, precum si necesitatea de tehnologii de protecție activa, sunt motivele ce au condus la introducerea in domeniu de noi tehnologii.

Pentru a se lua decizii rapide si optime este necesară o sporire a operativitatii, in colectarea, prelucrarea si prezentarea informațiilor precum si o valorificare superioara a acestora. Aceasta cerinta nu poate fi satisfacuta in condițiile unui volum din ce in ce mai mare de informații decat prin folosirea mijloacelor si tehnicilor specifice informaticii.

Securitatea sistemului informațional trebuie să fie o responsabilitate asumată de către structurile de conducere ale oricărei organizații din mediul privat sau public. Structurile de conducere trebuie să asigure o direcţie clară şi gestionată corespunzator pentru indeplinirea obiectivelor stabilite prinpolitica de securitate.

SECURITY BY DESIGN

Conceptul de „security by design” este foarte bun atunci când posibilităţile de implementare sunt justificate. De multe ori totuşi acest concept impune unele restricţii care limitează foarte mult utilizarea sa în arii diferite, metoda fiind folosită în zone speciale, foarte specializate (zone cu statut de importanţă majoră, ca de ex. reţelele de calculatoare care controlează traficul aerian, laboratoare de cercetare, etc.), zone în care accesul prin definiţie este foarte restrictiv.

Acest concept aplicat la „nivel software” generează un principiu de funcţionare al aplicaţiei cu restricţii foarte clare şi puternice – care de multe ori din pricina acestor limitări devine în scurt timp inutil.

IN-DEPTH SECURITY

„In-depth security” sau „defence in depth” este un principiu bazat pe mai multe „straturi” de securitate în vederea protejării sistemului sau reţelei din care face parte.

Trebuie să se înţeleagă că nu contează cât de de bun este fiecare „strat” – privit singular, există cineva mai deştept, cu resurse materiale şi temporale suficiente cât să treacă de acesta. Acesta este motivul pentru care practicile uzuale de securitate sugerează existenţa mai multor nivele de securitate sau pe scurt „in-depth security”.

Folosirea de nivele(layers) diferite de protecţie, de la diferiţi producători oferă o protecţie substanţial mai bună.

FIREWALL

DEFINIȚIE

O definiție a unui sistem de protecție tip Firewall ar putea fi: un sistem capabil sa implementeze politici de securitate pentru controlul accesului, in vederea restricționarii comunicațiilor la pe perimetrul dintre doua rețele. Traficul din interior şi spre exterior este filtrat, restricţionat, blocând eventualele transmisii nenecesare.

CUM FUNCȚIONEAZA?

De fapt, un firewall, lucrează îndeaproape cu un program de routare, examinează fiecare pachet de date din rețea (fie cea locală sau cea exterioară) ce va trece prin serverul gateway pentru a determina dacă va fi trimis mai departe spre destinaţie. Un firewall include de asemenea sau lucrează împreună cu un server proxy care face cereri de pachete în numele staţiilor de lucru ale utilizatorilor. În cele mai întâlnite cazuri aceste programe de protecţie sunt instalate pe calculatoare ce îndeplinesc numai această funcţie şi sunt instalate în faţa routerelor.
Astfel, un firewall este folosit pentru două scopuri:

- pentru a păstra în afara reţelei utilizatorii rău intenţionati (viruşi, viermi cybernetici, hackeri, crackeri)
- pentru a păstra utilizatorii locali (angajaţii, clienţii) în rețea

POLITICA FIREWALL-ULUI

Prin politica de securitate se înțelege un ansamblu de reguli (condiții si acțiuni) specificate, care trebuie aplicate pentru atingerea obiectivelor de securitate cerute

Înainte de a construi un firewall trebuie hotărâtă politica sa, pentru a şti care va fi funcţia sa şi în ce fel se va implementăa această funcţie.

Politica firewall-ului se poate alege urmând câţiva paşi simpli:

- alege ce servicii va deservi firewall-ul
- desemnează grupuri de utilizatori care vor fi protejaţi

- defineşte ce fel de protecţie are nevoie fiecare grup de utilizatori
- pentru serviciul fiecărui grup descrie cum acesta va fi protejat
- scrie o declaraţie prin care oricare alte forme de access sunt o ilegalitate

Politica va deveni tot mai complicată cu timpul, dar deocamdată este bine să fie simplă şi la obiect.

Această politică poate însemna:

- protejarea resurselor reţelei de restul utilizatorilor din alte reţele similare – Internetul -> sunt identificaţi posibilii "musafiri" nepoftiţi, atacurile lor asupra PC-ului sau reţelei locale putând fi oprite.
- controlul resurselor pe care le vor accesa utilizatorii locali.

CLASIFICARE

Firewall-urile pot fi clasificate după:

- Layerul (stratul) din stiva de reţea la care operează
- Modul de implementare

În funcţie de layerul din stiva TCP/IP (sau OSI) la care operează, firewall-urile pot fi:

- Layer 2 (MAC) şi 3 (datagram): packet filtering.
- Layer 4 (transport): tot packet filtering, dar se poate diferenţia între protocoalele de transport şi există opţiunea de "stateful firewall", în care sistemul ştie în orice moment care sunt principalele caracteristici ale următorului pachet aşteptat, evitând astfel o întreagă clasă de atacuri
- Layer 5 (application): application level firewall (există mai multe denumiri). În general se comportă ca un server proxy pentru diferite protocoale, analizând şi luând decizii pe baza cunoştinţelor despre aplicaţii şi a conţinutului conexiunilor. De exemplu, un server SMTP cu antivirus poate fi considerat application firewall pentru email.

Deşi nu este o distincţie prea corectă, firewall-urile se pot împărţi în două mari categorii, în funcţie de modul de implementare:

- dedicate, în care dispozitivul care rulează software-ul de filtrare este dedicat acestei operaţiuni şi este practic "inserat" în reţea (de obicei chiar după router). Are avantajul unei securităţi sporite.
- combinate cu alte facilităţi de networking. De exemplu, routerul poate servi şi pe post de firewall, iar în cazul reţelelor mici acelaşi calculator poate juca în acelaţi timp rolul de firewall, router, file/print server, etc.

Ce “poate” şi ce “nu poate” să facă un firewall?

Un firewall poate să:

- monitorizeze căile de pătrundere în reţeaua privată, permiţând în felul acesta o mai bună monitorizare a traficului şi deci o mai uşoară detectare a încercărilor de infiltrare;
- blocheze la un moment dat traficul în şi dinspre Internet;
- selecteze accesul în spaţiul privat pe baza informaţiilor conţinute în pachete.
- permită sau interzică accesul la reţeaua publică, de pe anumite staţii specificate;
- şi nu în cele din urmă, poate izola spaţiul privat de cel public şi realiza interfaţa între cele două.

De asemeni, o aplicaţie firewall nu poate:

- interzice importul/exportul de informaţii dăunătoare vehiculate ca urmare a acţiunii răutăcioase a unor utilizatori aparţinând spaţiului privat (ex: căsuţa poştală şi ataşamentele);
- interzice scurgerea de informaţii de pe alte căi care ocolesc firewall-ul (acces prin dial-up ce nu trece prin router);
- apăra reţeaua privată de utilizatorii ce folosesc sisteme fizice mobile de introducere a datelor în reţea (USB Stick, dischetă, CD, etc.)
- preveni manifestarea erorilor de proiectare ale aplicaţiilor ce realizează diverse servicii, precum şi punctele slabe ce decurg din exploatarea acestor greşeli.

Limitari

- fiabilitate redusa, din cauza implementării centralizate a acestui sistem
- posibila gatuire (en. bottleneck) a traficului
- necesita suport pentru asigurarea imunității sale la diverse categorii de atacuri (ex. DoS, atacul prin fragmentare IP, viruși/viermi);

ANTIVIRUS

DEFINIȚIE

Antivirusul este un program pe care-l instalați pe calculatorul personal pentru a-l proteja de infectarea cu malware. Termenul „malware“ este un termen generic, care desemnează orice tip de program software dăunător bunei funcționări a calculatorului, cum ar fi virușii, viermii, caii troieni sau programele de monitorizare spyware.

Problema este că antivirusul nu mai poate ține pasul cu ritmul atacatorilor cibernetici, aceștia dezvoltând și lansând constant noi tipuri de malware. Există atât de multe versiuni noi de malware lansate zilnic încât nici un program antivirus nu poate detecta și nu poate oferi protecție

pentru toate. Acesta este motivul pentru care este important să înțelegeți că, deși antivirusul ajută la protecția calculatorului personal, el nu poate detecta și stopa toate tipurile de malware.

Acestia ocupa resursele PC-ului (procesorul si memoria RAM) ducand astfel la incetinirea pornirii sistemului de operare si a programelor legitime ce pornesc odată cu el. Pe langa pagubele provocate, acestia reușesc sa se ascunda prin atașarea de cod unor fișiere de sistem iar la rularea acestora este executat inevitabil si virusul putand sa infecteze si alte fișiere. Un virus poate infecta un alt PC exclusiv prin mutarea unor fișiere infectate de pe un alt PC prin diferite moduri (transfer pe CD-compact disc, transfer pe rețea, stick de memorie, website-uri etc). Unii oameni folosesc termenul generic de virus pentru a se referi la orice program malitios si nu fac deosebiri. Termenul corect pentru orice program malițios este malware.

Un virus (informatic) este un program (software) ce se autocopiaza si infecteaza un PC fara permisiunea userului (utilizatorului). In cele mai multe cazuri acestea produc pagube precum ștergerea de fișiere, impiedicarea rularii programelor antivirus si a programelor legitime instalate si sunt si cazuri de formatare de partiții ale hard disk-ului.

CUM FUNCȚIONEAZA?

În general sunt două moduri în care un antivirus identifică un program malware: detecție pe bază de semnături și detecția bazată pe comportament.

DETECȚIA BAZATA PE SEMNATURI

Detecția pe bază de semnătură funcționează similar sistemului imunitar al omului. El scanează calculatorul pentru caracteristici sau semnături ale programelor cu funcționare dăunătoare cunoscute. Aceasta o face prin referirea la un dicționar de programe malware cunoscute: dacă ceva din calculator se potrivește cu unul din tiparele conținute în dicționar, antivirusul încearcă să-l neutralizeze. Asemeni sistemului imunitar uman, abordarea bazată pe dicționar necesită actualizări, cum sunt vaccinurile pentru gripă, ca să poată asigura protecția necesară față de noi versiuni de malware.

Antivirusul poate oferi protecție față de ceea ce poate recunoaște ca fiind periculos. Problema este că răufăcătorii dezvoltă noi versiuni de malware într-un ritm atât de rapid încât furnizorii de soluții antivirus nu reușesc să țină pasul cu ei Ca o consecință, indiferent cât de recent actualizat este programul antivirus, va exista întotdeauna o variantă de malware .care poate ocoli protecția oferită de antivirus. Deși este o componentă importantă a securității, antivirusul nu poate detecta și stopa toate atacurile.

DETECȚIE BAZATA PE COMPORTAMENT

Cu mecanismul de detecție bazat pe comportament antivirusul nu încercă să detecteze un program malware cunoscut ci monitorizează comportamentul în funcționare a programelor software instalate pe calculator. Atunci când un program are o funcționare suspectă, cum ar fi

încercarea de accesare a fișierelor protejate sau modificarea altui program, antivirusul detectează comportamentul suspect și vă alertează asupra acestuia.

Această abordare oferă protecție față de cele mai noi tipuri de malware care nu sunt încă incluse în niciun dicționar. Problema acestei abordări ,este că poate genera atenționări false. Dumneavoastră utilizatorul calculatorului, ați putea fi nesigur pe ce să permiteți sau nu și, în timp, să deveniți neutru față de toate aceste atenționări. Ați putea fi tentat să dați clic pe Acceptă“ la toate notificările, lăsând astfel calculatorul,, vulnerabil la atacuri și infectare. În plus, în momentul când comportamentul suspect este semnalat, programul malware cel mai probabil că este deja instalat și se execută pe calculatorul dumneavoastră și nu aveți de unde știi ce a .făcut până când a fost detectat de către antivirus. Indiferent de modul cum funcționează programul antivirus pe care-l folosiți, acesta nu vă poate proteja mereu față de orice tip de malware.

Eficienţa programelor antivirus poate fi redusă sau chiar anulată prin diverse moduri de atac, dintre care două sunt utilizate intens. Un virus de tip rootkit va înlocui fişierele sistemului de operare cu fişierele proprii „păcălind” astfel programul antivirus şi putând să-şi execute astfel propriul cod. Atacarea fişierelor AV presupune înlocuirea executabilelor programului antivirus sau alterarea dicţionarului de semnături.

ZONA DMZ

DEFINIȚIE

DMZ este un termen folosit pentru identificarea unei zone dintr-o reţea în care politica de securitate este permisivă (demilitarizată). O Zonă Demilitarizată (DMZ) este o arhitectură conceptuală de reţea în care serverele cu acces public sunt plasate separat pe un segment izolat de reţea. Scopul DMZ este acela de a asigura că serverele accesibile publicului nu pot intra în contact cu alte segmente interne de reţea, în situaţia în care un server este compromis.

Un firewall este deosebit de relevant în implementarea DMZ, din moment ce acesta este responsabil de punerea în aplicare a politicilor adecvate pentru a proteja reţelele locale de DMZ, în timp ce este menţinută accesibilitatea în DMZ.

Datorită naturii extraordinare a implementării DMZ, nu este recomandat să încercaţi această soluţie decât dacă deţineţi cunoştinţe solide de networking. DMZ-ul nu este în general o necesitate, dar este agreat de administratorii de reţea preocupaţi de securitate.

CUM FUNCȚIONEAZA?

DMZ este configurată pe un router sau un firewall şi funcţionează după următorul principiu: dacă ai o reţea privată cu conexiune la Internet, vei dori ca sistemele tale să poată accesa serviciile (sau doar anumite servicii) existente în reţeaua globală dar nu şi invers. Comunicarea între calculatorare se face prin trimiterea de solicitări către anumite servere şi primirea unor răspunsuri.

În mod normal calculatoarele din reţeaua ta vor accesa servicii din Internet trimiţând solicitări şi primind răspunsuri la acestea. Pot exista şi cazuri când reţeaua ta deţine un server public, adică un server care răspunde solicitărilor primite din afară (website, mail, FTP, etc). Având în vedere că de această dată vei primi solicitări la care trebuie să răspunzi, vei vrea să te asiguri că serverul este singurul care primeşte cereri din Internet, nu şi calculatoarele private întrucât ţi-ai asuma un risc de securitate.

În cazul de faţă poţi spune că serverul tău se află în DMZ. 3-leg perimeter presupune crearea unei reţele speciale separate pentru DMZ. În majoritatea cazurilor router-ul sau firewall-ul are 2 reţele conectate: reţeaua locală şi Internet-ul. 3-leg înseamnă că mai creezi o a treia conexiune în scopul prezentat mai sus.

MSBA

Este un program usor de folosit, dezvoltat de Microsoft, care are ca scop, detectarea slabiciunilor de securitate și detectarea acutulizarilor lipsa ale securității pentru urmatorele programe

- Client Version of Windows (Windows 7 inclusiv)
- Windows Server (Windows Server 2008 inclusiv)
- SQL Server
- Internet Server
- Microsoft Office

MSBA creează și stocheaza rapoarte individuale de securitate pentru fiecare calculator scanat. Aceste rapoarte sunt expuse in HTML și nu includ doar recomandari si informații despre nivelul de securitate, dar și detalii despre testele esuate și despre masurile corective recomandate.
Chiar daca rețeaua este actualizata la zi MSBA poate raporta o multitudine de erori. Nu este necesar sa rezolvam fiecare problema din aceste rapoarte . Anumite vulnerabilități raportate prezinta un risc redus pentru anumite sisteme. Totuși chiar daca MSBA nu raporteaza nici o problema asta nu inseamna ca sistemul nu este perfect funcțional.
Scanarea poate cauta doar anumite vulnerabilitati, totodata dupa ce instalam/actualizam anumite programe este recomandat sa rulam scanare MSBA ca sa ne asiguram ca pachetele de date descarcate au fost instalate corespunzator și ca nu exista probleme cu aceste.

IDS INTRUSION DETECTION SYSTEM

DEFINIȚIE

Un sistem de detectie al intruziunilor - IDS (Intrusion Detection System) reprezinta un echipament (sau o aplicație) care monitorizeaza activitațile rețelei si/sau sistemului cautand activitati malitioase sau violari ale politicilor.
Detecția intruziunilor este procesul de monitorizare a evenimentelor care au loc intr-un sistem sau o rețea de calculatoare si analiza lor pentru a detecta posibile incidente care sunt violari sau amenințari iminente de violare a politicilor de securitate, a politicilor de utilizare acceptate sau a practicilor standard de securitate.

Prevenirea intruziunilor este procesul prin care se desfasoara detecția intruziunilor si incercarea de inlaturare a posibilelor incidente detectate. Sistemele de detecție si prevenire ale intruziunilor - IDPS (Intrusion Detection-Prevention Systems) au ca scop principal identificarea posibilelor incidente, inregistrarea informațiilor despre ele, incercarea de inlaturare a incidentelor si raportarea catre administratorii de securitate.

In plus, organizatiile pot folosi IDPS-urile si pentru alte scopuri: identificarea problemelor legate de politicile de securitate, documentarea amenințarilor existente si descurajarea indivizilor in a incalca politicile de securitate.

Tipuri de IDS-uri

Sistem de detecție al intruziunilor de tip network-based

Intr-un sistem de detecție al intruziunilor de tip network-based - Network-based Intrusion Detection System (NIDS) - senzorii sunt localizați in puncte critice ale rețelei care este monitorizata, de cele mai multe ori la marginea rețelei sau in DMZ (demilitarized zone). Senzorii capteaza tot traficul din rețea si analizeaza conținutul fiecarui pachet cautand urme de trafic malitios.
Un NIDS reprezinta o platforma independenta care identifica intruziunile prin examinarea traficului din rețea si monitorizeaza mai multe statii. NIDS-urile pot vizualiza traficul din rețea prin conectarea lor la un hub sau la un echipament switch configurat cu port mirroring.

Sistem de detecție al intruziunilor de tip host-based

Intr-un sistem de detecție al intruziunilor de tip host-based - Host-based Intrusion Detection System (HIDS) - senzorul consta, de obicei, intr-un agent software care monitorizează toată activitatea ce se desfasoara pe stația pe care este instalat, incluzand aici sistemul de fișiere, kernel-ul si chiar aplicații in unele cazuri.

FUNCȚIONARE

Sistemele de detecție ale intruziunilor folosesc cel putin una dintre cele doua tehnici de detecție: anomalii statice si/sau semnaturi.

IDS bazat pe anomalii statice

- Un astfel de IDS stabileste o valoare inițiala de performanța bazata pe evaluari ale traficului normal din rețea. Dupa efectuarea acestui pas initial, IDS-ul va raporta traficul curent din rețea la valoarea inițiala stabilita pentru a stabili daca se incadreaza in limitele normale. Daca traficul din rețea depașește limitele normale va fi generata o alarma.

IDS bazat pe semnaturi

- Un astfel de IDS examineaza traficul din rețea cautand modele de atac preconfigurate si predeterminate cunoscute sub numele de semnaturi. Multe atacuri astazi au semnaturi diferite. Pentru a putea face fața amenințarilor o colectie de astfel de semnaturi trebuie actualizata in permanență.

IPS *INTRUSION PREVENTION SYSTEM*

DEFINIȚIE

Un Sistem de Prevenire al reprezinta un echipament de securitate al rețelei care monitorizeaza activitațile rețelei si/sau sistemelor si poate reactiona, in timp real, sa blocheze sau sa previna unele activitati malitioase.

Tehnologia prevenirii intruziunilor este vazuta de catre unii ca o extensie a tehnologiei de detecție a intruziunilor, deoarece un IPS trebuie sa fie in același timp si un foarte bun IDS pentru a asigura o rata scazuta de alarme false.

Un IPS este, in mod obisnuit, conceput pentru a opera complet invizibil in rețea. Produsele IPS nu au de obicei o adresa IP din rețeaua protejata dar pot raspunde in mod direct oricarui tip de trafic prin diverse metode (terminarea conexiunilor, renuntarea la pachete, generarea de alerte, etc.)
Desi unele IPS-uri au abilitatea de a implementa reguli de firewall aceasta este de obicei o funcție aditionala si nu una din funcțiile de baza ale produsului. Mai mult, tehnologia IPS ofera o mai bună monitorizare a operatiilor unei rețele furnizand informatii despre statiile active, incercarile de autentificare esuate, conținut necorespunzator si alte funcții ale nivelelor rețea si aplicație

Diferențe față de IDS-uri

IPS-urile au unele avantaje față de IDS-uri. Unul dintre acestea se refera la faptul ca IPS-urile sunt proiectate sa fie implementate in-line astfel incat tot traficul sa treaca prin ele si sa poata preveni atacurile in timp real. In plus, multe dintre soluțiile IPS au capabilitatea sa decodifice protocoalele de nivel aplicație (HTTP, FTP, SMTP) oferind astfel o mai bună monitorizare. Totuși atunci cand se doreste implementarea unui IPS de tip network-based trebuie sa se ia in considerare faptul ca daca prin respectivul segment de rețea circula trafic criptat majoritatea produselor nu pot sa inspecteze astfel de trafic.
Un alt avantaj major ar fi faptul ca unele dintre IPS-uri au posibilitatea de a corecta unele dintre metodele de evitare ale IDS-urilor(atacuri de tip DoS, inserarea de trafic).

Tipuri de IPS-uri Host-based

Un Sistem de Prevenire al Intruziunilor este de tip host-based (HIPS) atunci cand aplicația de prevenire a intruziunilor se afla pe adresa IP specifica sistemului protejat, de obicei o singura stație. HIPS complementează metodele antivirus traditionale bazate pe semnaturi deoarece nu necesita o actualizare continua pentru a putea raspunde atacurilor. Deoarece codul daunator trebuie sa modifice sistemul sau alte componente software care se afla pe masina in cauza un HIPS va observa aceste modificari si va incerca sa previna aceasta actiune sau sa anunte utilizatorul pentru permisiune.

Dezavantajul major al unui astfel de produs consta in folosirea extensiva a resurselor stației pe care se afla..

Network-based

Un Sistem de Prevenire al Intruziunilor este de tip network-based (NIPS) atunci cand aplicația/echipamentul de prevenire al intruziunilor se afla la o alta adresa IP decat stația pe care o monitorizeaza. NIPS sunt platforme hardware/software care analizeaza, detecteaza si raporteaza evenimente legate de securitatea unei rețele/segment de rețea de calculatoare.

LUCRARE DE LABORATOR
Scanare personalizată

Pentru a configura o scanare antimalware în detaliu și pentru a o lansa, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender.

2. În panoul Antivirus, faceți clic pe Scanează acum și selectați Administrare Scanări din meniul derulant.

3. Faceți clic pe Activitate nouă personalizată pentru a introduce o denumire pentru scanare și pentru a selecta locațiile ce urmează a fi scanate.

4. Dacă doriți să configurați opțiunile de scanare în detaliu, selectați tabul Avansat.Va apărea o nouă fereastră.Urmați acești pași:

a. Puteți configura ușor opțiunile de scanare reglând nivelul de scanare.

Utilizați descrierea din partea dreaptă a scalei pentru a identifica nivelul de scanare care se potrivește mai bine nevoilor dumneavoastră.

Utilizatorii avansați pot beneficia în urma ofertelor Bitdefender în ceea ce privește setările de scanare.Pentru a configura în detaliu opțiunile de scanare, faceți clic pe Personalizare. La sfârșitul acestei secțiuni, veți găsi informații privitoare la acestea.

b. De asemenea, puteți configura aceste opțiuni generale:

● Rulează sarcina cu prioritate scăzută . Reduce prioritatea procesului de scanare. Veți permite altor programe să ruleze cu o viteză superioară, dar timpul necesar pentru finalizarea scanării va crește.
● Minimizează Asistent de scanare în bara de sistem . Minimizează fereastra de scanare în bara de sistem. Faceți dublu-clic pe simbolul Bitdefender pentru a o deschide.
● Specificați acțiunea care trebuie luată în cazul în care nu sunt identificate niciun fel de amenințări

c. Faceți clic pe OK pentru a salva modificările și închide fereastra.

5. Faceți clic pe Programare dacă doriți să setați un program pentru sarcina de scanare.Folosiți butonul corespunzător pentru a activa sau dezactiva Programarea.Selectați una dintre opțiunile corespunzătoare pentru a seta un program:

● La pornirea sistemului
● O singură dată
● Periodic

6. Faceți clic pe Pornire scanare și urmați instrucțiunile asistentului de scanare antivirus pentru a finaliza operația de scanare.Procesul de scanare poate dura ceva timp, în funcție de locațiile ce vor fi scanate.După finalizarea scanării, vi se va cere să selectați acțiunile ce vor fi aplicate în cazul fișierelor detectate, dacă este cazul.

7. Dacă doriți, puteți relua rapid rularea scanării personalizate anterioare, făcând clic pe înregistrarea corespunzătoare din lista valabilă.

TEST

1.Cum identifica antivirusul un program malware?
a) Detecție pe baza de semnaturi
b) Detecție bazată pe comportament
c) Cu ajutorul firewall-ului
d) Prin detecția bazată atat pe semnaturi cat si pe comportament
e) Cu ajutorul zone DMZ
2. Unde este configurata zona DMZ?

a) Pe un firewall
b) Pe un firewall sau pe un router
c) Doar pe un router
d) In folderul windows
e) In baza de date a unui antivirus

3. De catre cine a fost dezvlotat programul MSBA?
a) Microsoft
b) Apple
c) Google
d) Alpha Software
e) SoftWorks

4. Unde sunt expuse rapoartele MSBA?
a) In folderul MSBA
b) In folderul Windows
c) In HTML
d) Pe site-ul MSBA
e) Nicăieri

5. Ce fel de sistem de detecție al intruziunilor este IDS-ul?
a) Host-based
b) Online
c) Port mirroring
d) SMTP
e) Network-based

6. Un ansamblu de componente hardware (dispozitive) si componente software (sistem de operare si programe specializate) ce ofera servicii utilizatorului pentru coordonarea si controlul executarii operațiilor prin intermediul programelor se numeste:
a) Sistem de calcul
b) Windows
c) Antivirus
d) Firewall
e) Driver

7. Traficul din interiorul şi spre exteriorul unei rețele este filtrat, restricţionat, blocând eventualele transmisii nenecesare, de catre:
a) Antivirus
b) Firewall
c) IDS/IPS
d) MSBA
e) Un server proxy

8. Un program (software) ce se autocopiaza si infecteaza un PC –ul fara permisiunea userului (utilizatorului) se numeste
a) Driver
b) Windows
c) Server
d) Torrent
e) Virus

9. Ce face un virus de tip rootkit?

a) Ne inchide PC-ul
b) Ne cripteaza informațiile in scopul de a ne limita accesul la acestea
c) Inlocuiește fișierele sistemului de operare cu fişierele proprii „păcălind” astfel programul antivirus şi putând să-şi execute astfel propriul cod.
d) Nu ne afecteaza cu nimic
e) Fura informații cu privire la actiunile efectuate de tastatură

10. Care este scopul zonei DMZ?
a) De a ne mari performanțele PC-ului
b) De a efectua anumite sarcini pentru noi
c) De a cauta update-uri pentru Windows
d) De a se asigura că serverele accesibile publicului nu pot intra în contact cu alte segmente interne de reţea
e) De a se asigura ca un calculator nu poate avea o conexiune sigură la internet

11. Cum se conecteaza un PC din reteaua personala la unele servicii de internet?
a) Trimițând solicitari si primind raspunsuri la acestea
b) Accesand registrele windows
c) Conectandu-se la un server privat
d) Cu ajutorul altor programe
e) Prin rețeaua publica

12. Ce scop are scanarea MSBA?
a) De a descoperi virusi
b) De a ne intari reteaua
c) De a gasi vulnerabilitați in securitate si de a se asigura de instalarea corecta a pachetelor
d) De a cauta metode de distrugere a virusilor
e) De a ne proteja impotriva atacurilor informatice

13. Cum functioneaza IDS-ul?
a) Cu ajutorul anomaliilor statice
b) Cu ajutorul anomaliilor statice si al semnaturilor
c) Doar cu ajutorul semnaturilor
d) Cu ajutormul zonei DMZ
e) Prin alte metode

14. Cand este un sistem de prevenire al intruziunilor este de tip network-based (NIPS)?
a) Atunci cand aplicația de prevenire a intruziunilor se afla pe aceiasi adresa IP pe care o monitorizeaza
b) Atunci aplicația nu este asociata unei adrese IP
c) Atunci cand aplicația supravegheaza sursa de pe mai multe adrese IP
d) Atunci cand aplicația de prevenire a intruziunilor se afla pe alta adresa IP față ce cea pe care o monitorizeaza
e) Un astfel de sistem nu poate fi de tip network-based

15. Unde se aplica conceptul de „security by design”?
a) Unei aplicații cu restrictii clare
b) Unui soft dezvoltat exclusiv pentru acest lucru
c) La nivel hardware
d) La nivel atat hardware cat si software
e) La nivel software

1-d	6-a	11-a
2-b	7-b	12-c
3-a	8-e	13-b
4-c	9-c	14-d
5-e	10-d	15-e

BIBLIOGRAFIE

1) J. H. Saltzer, M. D. Schroeder.

- "The protection of information in computer systems"

2) Matt Bishop

- Files and Security Flaws
- Overview of Computer Security

3) Dabija George

- Securitatea sistemelor de calcul şi a reţelelor de calculatoare