HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Microsoft Baseline Security Analyzer

CCERT-PUBDOC-2003-01-02

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Microsoft® Baseline Security Analyzer (MBSA) programski je paket koji omogućuje pregledavanje jednog ili skupine Windows računala s obzirom na različite tipove ranjivosti.
Dosadašnja iskustva u radu s Windows operacijskim sustavima pokazala su da je sigurnost jedan od najvećih nedostataka Microsoftovih proizvoda. Ideja Microsofta da se korisniku što više pojednostavni postupke administracije te da se što više postupaka automatizira, dovela je do velikog broja sigurnosnih incidenata koji su posljedica upravo neispravne konfiguracije sustava.
Težnja za što bržim izbacivanjem novih proizvoda na tržište također je rezultirala velikim brojem sigurnosnih propusta koji neovlaštenim korisnicima otvaraju prostor za maliciozne radnje. Problemi ovog tipa danas se tipično rješavaju objavljivanjem različitih sigurnosnih zakrpi koje redom uklanjaju novo otkrivene propuste. Redovita instalacija sigurnosnih zakrpi danas je postala osnovni preduvjet za sigurnost računalnih sustava.
Mrežni sustavi s velikim brojem računala i s različitim tipovima Windows operacijskih sustava predstavljali su poseban problem za mrežne administratore. Problematika pravovremenog uočavanja novih sigurnosnih upozorenja (eng. *security advisories)* te pojedinačne instalacije zakrpi na svakom od računala negativno je utjecalo na brzinu procesa uklanjanja sigurnosnih nedostataka. Brzina kojom se danas pojavljuju i šire novi maliciozni programi (npr. *Nimda*, *Code Red*, *Klez* i brojni drugi crvi) dovoljno je velika da se zatekne iznimno velik broj nezaštićenih računala (u slučaju da ista nisu redovno održavana).
Shvativši ovu problematiku Microsoft je u posljednje vrijeme dao poseban naglasak na sigurnost svojih operacijskih sustava. MBSA samo je jedan od alata koji administratorima omogućuje analizu sustava sa stanovišta sigurnosti.
U nastavku dokumenta biti će opisane mogućnosti programa zajedno s načinom korištenja.

2. Zahtjevi

Korištenje MBSA programskog paketa postavlja neke osnovne zahtjeve pred računala na kojima se program pokreće i na računala koja se pregledavaju. Osnovni uvjet za provođenje testova je taj da korisnik koji pokreće program ima administratorske ovlasti na računalima koja se žele ispitivati. Bez prikladnih ovlasti program će odbiti nastavak testiranja.

2.1. Zahtjevi na računala na kojima se program pokreće

Na računalo na kojem se program pokreće predstavljaju se sljedeći zahtjevi:

- Windows 2000/XP operacijski sustav;
- Internet Explorer web preglednik, inačica 5.01 ili više;
- XML parser (MSXML Version 3.0 SP2). Ovaj paket moguće je odabrati prilikom instalacije programa, ukoliko isti nije već ranije instaliran. Na sustavima na kojima nije instaliran IE 5.01 ili više, potrebno je zasebno instalirati ovaj paket.
- Ukoliko se provode ispitivanja IIS poslužitelja potrebno je instalirati posebni skup specijalnih modula koji to omogućuju.

2.2. Zahtjevi na računala koja se pregledavaju

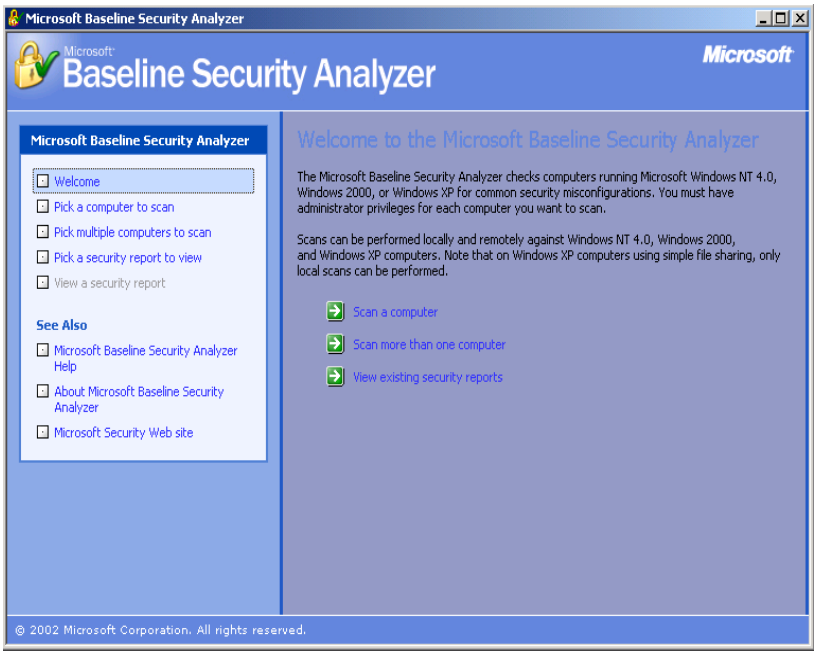
Zahtjevi na računala prema kojima je ispitivanje usmjereno su sljedeći:

- Windows NT 4.0 SP4 ili više, XP, 2000 operacijski sustavi;
- IIS 4.0/5.0 (ukoliko se provodi ispitivanje IIS poslužitelja);
- Internet Explorer web preglednik, inačica 5.01 ili više;
- SQL 7.0 ili 2000 (ukoliko se provodi ispitivanje SQL poslužitelja;
- Microsoft Office 2000/XP (ukoliko se provodi ispitivanje Microsoft Office paketa).

Korisnik koji provodi pregledavanje mora imati ovlasti administratora na računalima koja se pregledavaju. `Server` i `Remote Registry` servisi moraju biti pokrenuti na svim računalima koja se pregledavaju ovim putem. *Remote Registry* servis omogućuje udaljeno pregledavanje i uređivanje Windows *registry-a*, dok `Server` servis omogućuje dijeljenje datotečnog sustava i pisača.

3. Korištenje programa

Korisničko sučelje MBSA programa estetski je vrlo dotjerano i intuitivno, što u velikoj mjeri olakšava korištenje programa. Glavni prozor podijeljen je na dva dijela. Na lijevoj strani nalazi se sučelje za navigaciju kroz program, dok se s desne strane prikazuje sadržaj ovisno o odabranoj opciji.



Slika 1 *- Grafičko sučelje MBSA programskog paketa*

Nakon pokretanja programa korisniku se prikazuje sučelje prikazano na gornjoj slici. Korisniku su odmah ponuđene opcije pregledavanja jednog ili više računala ili pregledavanja izvještaja prethodnih ispitivanja. Odabirom jedne od opcija pregledavanja računala, korisnika se vodi kroz postupak definicije računala uključenih u pregledavanje.

Za svako ispitivanje moguće je osim IP adrese ili imena računala odabrati i grupu testova koji se žele provesti. O tipu testova koje je moguće provoditi MBSA programom biti će više riječi u sljedećem poglavlju (4).

Nakon definicije potrebnih parametara, uslijediti će sam postupak ispitivanja odabranog/ih računala, čije trajanje ponajviše ovisi o broju računala i opsežnosti odabranih testova.

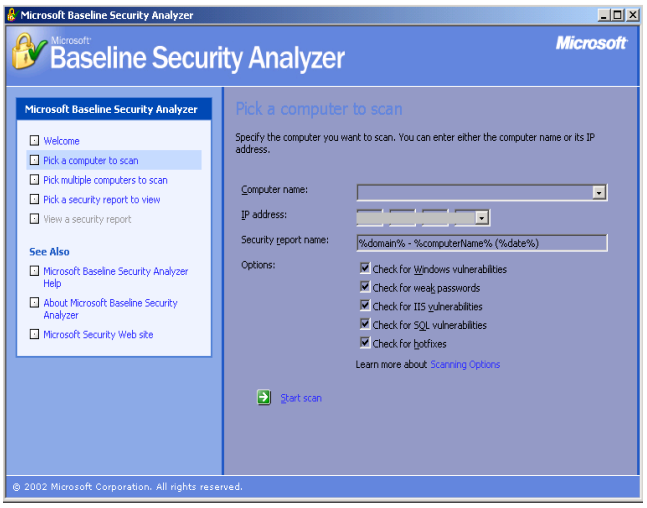
Nakon što je postupak testiranja završen, korisniku će biti prikazan izvještaj provedenih testova, koji je moguće pohraniti ili ispisati na pisaču. Više riječi o samom izvještaju biti će u jednom od narednih poglavlja (5).

4. Mogućnosti programa

U nastavku je dana lista mogućnosti MBSA programa s kratkim opisom svake od njih. Sve ranjivosti, odnosno propusti koje program provjerava kategorizirane su u nekoliko osnovnih skupina:

- Općenite Windows provjere
- IIS provjere
- SQL provjere
- Provjere korisničkih aplikacija

Koje će se od raspoloživih provjera provoditi moguće je odabrati prilikom samog pokretanja provjera.



***Slika 2**- Definiranje parametara pregledavanja računala*

Ovisno o tome da li je odabrano pregledavanje jednog ili više računala, potrebno je definirati odgovarajuće parametre (ime ili IP adresu računala), opsežnost testiranja te ime pod kojim će se generirati izvještaj.

4.1. Općenite Windows provjere

U kategoriju općenitih Windows provjera uključeni su sljedeći testovi:

4.1.1. Provjera instaliranih sigurnosnih i *hotfix* zakrpi

Sigurnosne zakrpe (eng. *Service pack*) su skup provjerenih i ispitanih zakrpi koje uklanjaju različite sigurnosne propuste kod nekog proizvoda. Sigurnosne zakrpe su kumulativne, što znači da svaka nova uključuje sve stare zakrpe, plus one novo objavljene.
Za razliku od sigurnosnih zakrpi, *hotfix* zakrpe su namijenjene točno jednom specifičnom sigurnosnom problemu. Skup *hotfix* zakrpi se nakon nekog perioda objavljuje u obliku *service pack* zakrpe, koja se prema ovom načelu može definirati kao skup dotada objavljenih *hotfix* zakrpi.
MBSA program će pokušati utvrditi sigurnosne i *hotfix* zakrpe koje nedostaju na ispitivanom računalu, zajedno s vezama na originalne Microsoftove dokumente u kojima je dan detaljniji opis svake od njih.

4.1.2. Zaporke s neograničenim trajanjem

Kao rezultat ovog testa biti će dana lista svih korisničkih računa na sustavu, kojima zaporka ima neograničeno trajanje.
Sa stanovišta sigurnosti preporučuje se korištenje zaporki s ograničenim trajanjem, kako bi se na taj način omogućilo učestalo mijenjanje zaporki.

4.1.3. Datotečni sustav

Analiziraju se tipovi datotečnog sustava na testiranom računalu. Ukoliko na testiranom sustavu nisu svi tvrdi diskovi, odnosno particije formatirane kao NTFS sustav, to će biti prijavljeno kao sigurnosno upozorenje.
NTFS sustav smatra se sigurnijim od FAT datotečnog sustava s obzirom na mogućnost postavljanja ovlasti pristupa, enkripcije datoteka i direktorija, kompresije i sl.

4.1.4. Provjeravanje Auto Logon opcije

Ovaj test uključuje provjeru da li je na sustavu omogućena *Auto Logon* opcija, i da li se korisnički parametri autentikacije u *registry*-u pohranjuju kriptirano ili u čistom tekstualnom obliku (eng. *plain text*).

Auto Logon opcija kod Windows operacijskih sustava omogućuje prijavljivanje u sustav bez zaporke. Iako je ova mogućnost u određenim situacijama vrlo korisna (npr. kada se računalo pokreće udaljeno), ona se također smatra sigurnosnim rizikom visokog prioriteta.
Da bi se omogućila ova opcija potrebno je u *registry*-u sustava, na lokaciji *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon* definirati ključ *AutoAdminLogon* i pridijeliti mu vrijednost jedan. Korisnička zaporka koju sustav koristi prilikom prijavljivanja u sustav definirana je parametrom *AutoAdminLogon*, i može biti pohranjena u čistom tekstualnom ili kriptiranom obliku.
Ukoliko je ova opcija omogućena i zaporka je pohranjena u čistom tekstualnom obliku ista će biti prijavljena kao propust visokog rizika.

4.1.5. Provjera Guest korisničkog računa

Provjerava se da li je na udaljenom računalu omogućen *Guest* korisnički račun. *Guest* korisnički račun upotrebljavaju oni korisnici koji se prijavljuju u sustav na kojem nemaju svoj vlastiti korisnički račun ili prilikom pristupa sustavu s domene kojoj se vjeruje (eng. *trusted domains*).
Na sustavu na kojem je omogućen *Guest* korisnički račun, isti će biti prijavljen kao sigurnosni rizik.

4.1.6. Anonimni pristup

Ovaj test provjerava da li je na sustavu omogućen anonimni pristup sistemskim resursima. Anonimni pristup sustavu omogućuje pregledavanje korisnika na sustavu, razne sistemske informacije, definiranu sigurnosnu politiku i sl.
Na računalima visokog prioriteta se iz sigurnosnih razloga preporučuje onemogućavanje anonimnog pristupa.
Registry ključ *RestrictAnonymous* definira nivo ovlasti koje donosi anonimni pristup sustavu. Moguće vrijednosti su:

- 0 - Inicijalne ovlasti;
- 1 - nije dozvoljeno pregledavanje SAM (eng. *Security Accounts Manager*) korisničkih računa i imena;
- 2 - bez ovlasti, osim ukoliko iste nisu eksplicitno definirane.

MBSA program će prijaviti ukoliko je na sustavu omogućen anonimni pristup sa neprikladnim ovlastima.

4.1.7. Provjera korisničkih računa s administratorskim ovlastima

Analiziraju se svi korisnički računi na sustavu koji imaju ovlasti lokalnog administratora. Ukoliko se detektira više od jednog korisničkog računa sa ovlastima lokalnog administratora, isti će biti prijavljeni, budući da se stanovišta sigurnosti preporučuje što manji broj korisničkih računa sa ovlastima administratora.

4.1.8. Provjera korisničkih računa bez zaporke

U ovaj test uključena je provjera sustava s obzirom na korisničke račune bez definirane zaporke, ili račune sa "slabijim" zaporkama. Prazne ili slabe zaporke posebno su opasne, budući da neovlaštenom korisniku omogućuju relativno jednostavan pristup sustavu.
Program će generirati upozorenje ukoliko neki od korisničkih računa nema definiranu zaporku, ukoliko ista odgovara korisničkom ili imenu računala, ili ukoliko je zaporka neki jednostavan niz (`administrator`, `admin`, `root` i sl.).

4.1.9. Provjera nepotrebnih servisa

Provjerava se stanje servisa navedenih u `services.txt` datoteci. `Services.txt` je konfiguracijska datoteka koja se instalira zajedno sa MBSA programom. Za svaki od servisa navedenih u ovoj datoteci provjerava se da li je isti omogućen ili ne.
Inicijalno se provjeravaju sljedeći servisi: `MSFTPSVC` (FTP), `TlntSvr` (Telnet), `RasMan` (*Remote Access Service Manager*), `W3SVC` (WWW), `SMTPSVC` (SMTP).

4.1.10. Dijeljeni direktoriji

Analiziraju se dijeljeni direktoriji na sustavu (eng. *shares*). Program će kao rezultat testa dati listu dijeljenih direktorija zajedno s njihovim imenima i ovlastima.

4.1.11. Bilježenje događaja

Ovaj test uključuje provjeru da li je na sustavu omogućeno bilježenje događaja (eng. *Windows Auditing*). *Windows Auditing* je servis Windows 2000 operacijskih sustava koji omogućuje praćenje i bilježenje aktivnosti na računalu putem *log* zapisa (*Event Log* servis).

4.1.12. Inačica operacijskog sustava

Zadnji test iz ove skupine određuje inačicu operacijskog sustava instaliranu na udaljenom računalu. Ovaj test može biti vrlo koristan za administratore, budući da je ovim putem vrlo jednostavno utvrditi tipove računala koja se nalaze na lokalnoj mreži.

4.2. IIS provjere

U ovu skupinu testova uključene su provjere vezane za Microsoft `Internet Information Server` poslužitelj. Slijedi kratki opis testova uključenih u ovu skupinu.

4.2.1. IIS Lockdown

Na samom početku provjerava se da li je na sustavu već ranijem pokrenut `IIS Lockdown` programski alat, koji dolazi kao dio `Microsoft Security Toolkit` programskog paketa. `IIS Lockdown` programski paket onemogućuje neke nepotrebne postavke unutar `IIS` poslužitelja koje unose dodatni sigurnosni rizik u sustav.
Ovim testom moguće je utvrditi i trenutno stanje konfiguracije `IIS` poslužitelja.

4.2.2. Inicijalne postavke `IIS` poslužitelja

Ovim testom želi se utvrditi da li su na poslužitelju ostavljene inicijalne postavke nakon instalacije poslužitelja. Provjeravaju se sljedeći direktoriji:

- `\Inetpub\iissamples`
- `\Winnt\help\iishelp`
- `\Program Files\Common Files\system\msadc`

`MBSA` program prijaviti će ukoliko su na poslužitelju ostavljene inicijalne postavke, budući da iste nepotrebno unose sigurnosni rizik u sustav.

4.2.3. Pristup direktorijima

Ovim testom provjerava se da li je na poslužitelju omogućena *ASPEnableParentPaths* opcija. Njenim omogućavanjem dozvoljava se ASP skriptama pristup direktorijima putem `..` niza znakova.
Ova opcija posebno je opasna budući da poslužitelj ostavlja otvorenim na tzv. *directory traversal* tipove napada. Tipični predstavnik malicioznih programa koji koriste ovu ranjivost je popularni *Nimda* crv.

4.2.4. Provjera instaliranih sigurnosnih i *hotfix* zakrpi

Slično kao i za sam operacijski sustav MBSA program provjerava instalirane zakrpe za `IIS` poslužitelj. `MBSA` program će kao rezultat testa dati listu sigurnosnih zakrpi koje nedostaju na sustavu.

4.2.5. Provjera IISADMPWD virtualnog direktorija

Ovaj test provjerava da li je na sustavu instaliran *IISADMPWD* virtualni direktorij. `Internet Information Server (IIS) 4.0` korisnicima omogućuje promjenu Windows zaporke te obavještavanje korisnika o njihovom isteku. *IISADMPWD* virtualni direktorij instalira se zajedno s `IIS 4.0` poslužiteljem i sadrži datoteke koje omogućuju navedene aktivnosti.

Opisana mogućnost implementirana je `.htr` datotekama koje se nalaze u `\System32\Inetsrv\Iisadmpwd` direktoriju te `Ism.dll` ISAPI nastavkom.
MBSA program će generirati upozorenje ukoliko je ova opcija omogućena, budući da se promjena zaporke putem Interneta smatra sigurnosnim rizikom.

4.2.6. Provjera MSADC i Scripts virtualnog direktorija

Ovim testom provjerava se da li su na sustavu instalirani *MSADC* i *Scripts* virtualni direktoriji. Spomenuti direktoriji sadrže test skripte koje se u većini slučajeva mogu ukloniti sa sustava.
Ukoliko spomenuti direktoriju nisu neophodni preporučuje se njihovo uklanjanje sa sustava. Neki od popularnih napada (npr. *Nimda* crv) koristili su upravo propuste unutar spomenutih direktorija u kombinaciji s *Directory Traversal* ranjivostima.

4.2.7. Log zapisi

Sljedeći test provjerava da li je unutar `IIS` poslužitelja omogućeno bilježenje log zapisa i da li se zapisi bilježe u standardnom *W3C Extended Log* formatu.
`IIS` omogućuje praćenje i bilježenje različitih događaja vezanih uz pristup web poslužitelju. Moguće je kontrolirati vrijeme pristupa, kojem se resursu pristupa i od kuda, da li je pristup bio uspješan ili neuspješan te slične ostale informacije.
Kontinuirano bilježenje zapisa te njihova redovita analiza jedan je od temelja računalne sigurnosti. Ukoliko ova mogućnost na sustavu nije omogućena MBSA program će to prijaviti.

4.2.8. IIS poslužitelj instaliran na poslužitelju domene

Zadnjim testom iz ove skupine provjerava se da li je IIS poslužitelj instaliran na poslužitelju domene (eng. *Domain Controller*). S obzirom na važnost podataka koji se nalaze na poslužitelju domene iz sigurnosnih razloga nikako se ne preporučuje instalacija IIS poslužitelja na istom računalu.
Ukoliko MBSA program detektira računalo na kojem je instaliran IIS poslužitelj, a istovremeno je i poslužitelj domene, biti će prijavljeno upozorenje visokog sigurnosnog rizika.

4.3. SQL provjere

4.3.1. Pripadnost Administrators grupe

Prvim testom ove skupine provjerava se da li *Administrators* grupa sustava pripada *SysAdmin* grupi SQL poslužitelja. *SysAdmin* SQL grupa je skup korisničkih računa koji imaju administratorske ovlasti nad poslužiteljem.
Inicijalna instalacija poslužitelja *Administrators* grupu korisnika automatska stavlja u *Sysadmin* grupu.

4.3.2. Ograničavanje CmdExec ovlasti

Ovim testom provjerava se da li su *CmdExec* ovlasti ograničene samo na administratora sustava. Svi ostali korisnički računi s *CmdExec* ovlastima biti će prijavljeni kao sigurnosno upozorenje.

4.3.3. SQL poslužitelj instaliran na poslužitelju domene

Slijedećim testom iz ove skupine provjerava se da li je SQL poslužitelj instaliran na poslužitelju domene (eng. *Domain Controller*). S obzirom na važnost podataka koji se nalaze na poslužitelju domene, iz sigurnosnih razloga nikako se ne preporučuje instalacija SQL poslužitelja na istom računalu.
Ukoliko MBSA program detektira računalo na kojem je instaliran SQL poslužitelj, a istovremeno je i poslužitelj domene, biti će prijavljeno upozorenje visokog sigurnosnog rizika.

4.3.4. Provjera zaporke sa korisničkog računa

Provjerava se da li je zaporka `sa` (*System Administrator*) korisničkog računa unutar `%temp%\sqlstp.log` i `%temp%\setup.iss` datoteka pohranjena u čistom tekstualnom

obliku. Ukoliko se za instalaciju SQL 7.0 sigurnosnih zakrpi koristi *SQL Server Authentication* (*Standard Security*) servis, zaporka `sa` korisnika je u spomenutim datotekama pohranjena u čistom tekstualnom obliku.
MBSA će prijaviti ovaj propust ukoliko se isti primijeti na testiranom računalu.

4.3.5. Ovlast pristupa SQL direktorijima

Analiziraju se prava pristupima pojedinim SQL direktorijima, kako bi se utvrdilo da li su ograničena na korisničke račune SQL servisa i lokalnog administratora. Analiziraju se sljedeći SQL direktoriji:

- `Program Files\Microsoft SQL Server\MSSQL$InstanceName\Binn`
- `Program Files\Microsoft SQL Server\MSSQL$InstanceName\Data`
- `Program Files\Microsoft SQL Server\MSSQL\Binn`
- `Program Files\Microsoft SQL Server\MSSQL\Dana`

MBSA program provjerava ovlasti pristupa navedenim direktorijima putem ACL (eng. *Access Control List*) listi te prijavljuje sve korisničke račune za koje se smatra da to nije potrebno.

4.3.6. Ovlasti Guest korisničkog računa

Ovom provjerom analizira se da li *Guest* korisnički račun ima prava pristupa SQL bazama podataka, osim `master`, `tempdb` i `msdb` baza. Sve ostale baze kojima *Guest* korisnički račun ima pristup prijavljene su u izvještaju kao sigurnosno upozorenje.

4.3.7. Ovlasti Everyone korisničke grupe

Provjerava se da li su korisnici *Everyone* grupe ograničeni samo na ovlasti čitanja (eng. *read*) sljedećih *registry* zapisa:

- `HKLM\Software\Microsoft\Microsoft SQL Server`
- `HKLM\Software\Microsoft\MSSQLServer`

Ukoliko korisnici *Everyone* grupe imaju veće ovlasti od ovlasti čitanja biti će prijavljeno upozorenje.

4.3.8. Provjera servisnih SQL korisničkih računa

Provjerava se da li SQL korisnički računi pripadaju grupi lokalnog ili administratora domena i da li se neki od istih računa koristi u *LocalSecurity* kontekstu. U testiranje su uključeni *MSSQLServer* i *SQLServerAgent* SQL korisnički računi.

4.3.9. Prazne zaporke

Ovim testom pokušava se utvrditi da li neki od SQL korisničkih računa ima praznu zaporku, odnosno da li su zaporke previše jednostavne. Jednostavne zaporke smatraju se jednako opasnima kao da ih nema uopće.
U okviru testova biti će prijavljeni svi korisnički računi sa sljedećim karakteristikama:

- zaporka nije definirana;
- zaporka je jednaka korisničkom imenu;
- zaporka je jednaka imenu računala;
- zaporka koristi riječ `password`;
- zaporka koristi riječ `sa`;
- Zaporka koristi riječi poput `administrator`, `admin` i sl.

4.3.10. SQL autentikacija

Utvrđuje se metoda SQL autentikacije na poslužitelju koji se testira. SQL poslužitelj podržava dvije osnovne metode autentikacije za kontrolu pristupa poslužitelju:

- *Windows Authentication Mode* – autentikaciju korisnika provodi se na razini Windows operacijskog sustava.
- *Mixed Mode* – Ukoliko jedan od sudionika ne podražava Windows metode autentikacije (Kerberos, NTLM), autentikaciju provodi sam SQL poslužitelj na temelju svojih parametara (korisničkog imena i zaporke) pohranjenih u internim tablicama.

4.3.11. Pripadnost Sysadmin grupi

Zadnjim testom ove skupine provjeravaju se članovi koji pripadaju *SysAdmin* grupi (eng. *role*) korisnika. SQL poslužitelj koristi tzv. *role* grupe za grupiranje korisnika s istim ovlastima. *Sysadmin* grupa svim svojim korisnicima daje ovlasti administratora sustava.
MBSA program prijaviti će sve korisnike koji pripadaju ovoj grupi te upozoriti na potencijalne probleme.

4.4. Provjere ostalih aplikacija

4.4.1. Sigurnosne postavke IE zona

Ovim testom provjeravaju se sigurnosne postavke `Internet Explorer` web preglednika. Provjeravaju se definirane Internet zone za svakog lokalnog korisnika.
Unutar `IE` web preglednika moguće je definirati različite postavke za različite Internet zone (*Tools -> Internet Options -> Security*).
Inicijalne postavke programa moguće je prilagoditi osobnim potrebama, čime se može podići sigurnosni nivo sustava.
MBSA program će detektirati ukoliko su na sustavu modificirane inicijalne postavke, ali ne može utvrditi da li su iste pouzdanije od onih inicijalnih.

4.4.2. Sigurnosne postavke MS Outlooka

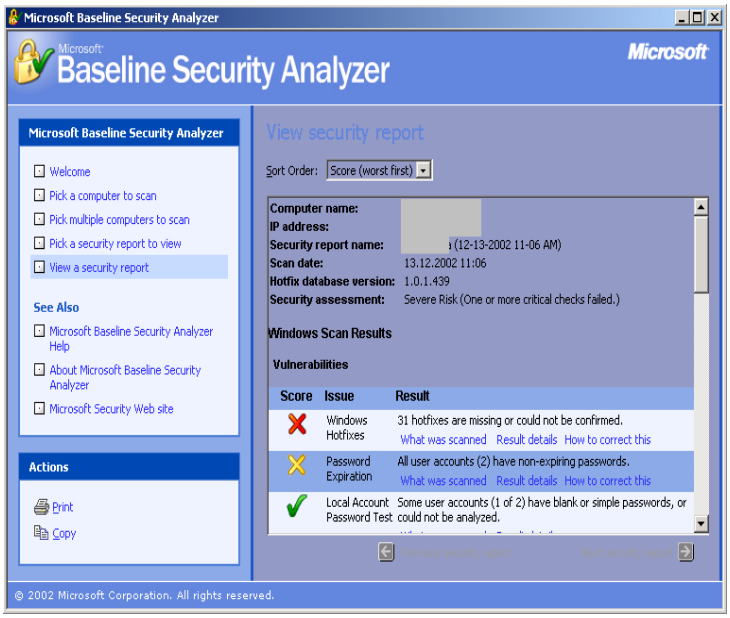
Slično kao i za `IE` programski paket, ovim testom analiziraju se sigurnosne postavke `MS Outlook` klijentskog programa. Nakon instalacije MS Outlook programa podešene su inicijalne sigurnosne postavke programa.
Modifikacijom ovih parametara (*Tools -> Options*) moguće je podići sigurnosni nivo sustava, tako da se ograniče mogućosti programa prilikom procesiranja poruka elektroničke pošte.

4.4.3. Dozvole izvršavanja makro programa

Zadnjom provjerom analiziraju se sigurnosne postavke *MS Office* alata s obzirom na mogućnosti izvršavanja makro programa. Neispravne postavke programa vezane za izvršavanje makro programa mogu ozbiljno utjecati na sigurnost sustava.
MBSA program će analizirati sljedeće programe: `Word`, `Excel`, `PowerPoint` i `Outlook`.

5. Izvještaj

Nakon što je završen postupak testiranja, MBSA program će generirati izvještaj obavljene provjere (Slika 3). Izvještaj se generira u XML formatu i korisniku se prikazuje u HTML formatu unutar glavnog prozora.



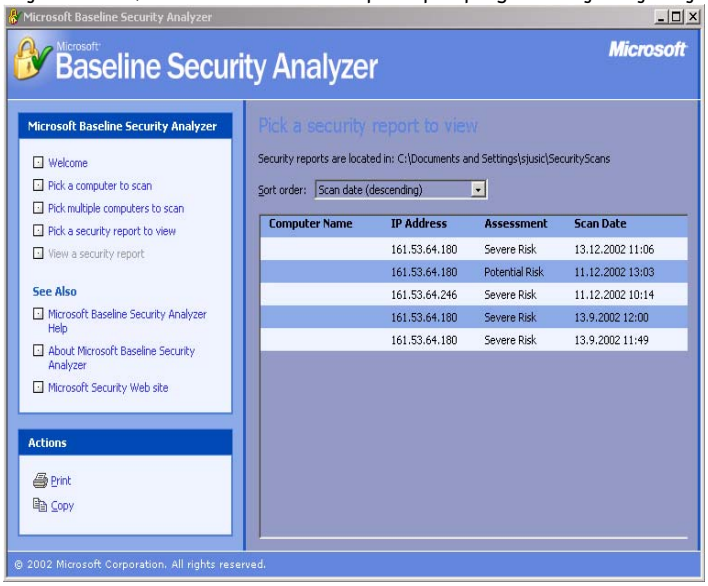
Slika 3 *- Izvještaj MBSA programa*

Izvještaj testiranja vrlo je pregledan i dobro organiziran. Za svaki otkriveni propust označen je pripadajući prioritet, dan je kratki opis problema, rezultat testiranja te načini kako je moguće ukloniti problem.

Na primjer, ukoliko na sustavu nisu instalirane odgovarajuće sigurnosne zakrpe, pritiskom na vezu *Result Details*, moguće je dobiti listu svih zakrpi koje nisu instalirane, zajedno s vezama na originalne dokumente koji detaljnije opisuju problematiku vezanu za svaku od njih.

Pri samom vrhu prozora moguće je odabrati način sortiranja detektiranih ranjivosti. Moguće je odabrati prikaz prema imenu ranjivosti i prema nivou sigurnosnog rizika (padajućem i rastućem).

Unutar lijevog prozora programa moguće je pritiskom na vezu *Pick a security report to view,* dobiti listu svih dosadašnjih testova, što dodatno olakšava postupak pregledavanje izvještaja (Slika 4).



Slika 4 *- Lista izvještaja MBSA programa*

Vezano za način generiranja izvještaja MBSA programa, nekoliko je sigurnosnih organizacija objavilo dokument kojim se upozorava na potencijalnu ranjivost.

Naime, svi izvještaji MBSA programa pohranjuju se unutar `C:\Documents and Settings\<korisnicko_ime>\SecurityScans\` direktorija u čistom tekstualnom obliku. Budući da izvještaji programa sadrže iznimno povjerljive podatke o ranjivostima testiranih računala, njihovo otkrivanje predstavljalo bi veliku opasnost za sustav.
Microsoftu je prijavljen ovaj problem i u sljedećim inačicama programa očekuje se njegovo uklanjanje.

6. Pokretanje putem naredbenog retka

Osim putem grafičkog sučelja program je moguće koristiti i putem naredbenog retka. Program se pokreće zadavanjem naredbe `mbsacli.exe`. Način rada programa može se kontrolirati zadavanjem odgovarajućih parametara koji su opisani u nastavku poglavlja.

6.1.1. Odabir računala

Odabir računala uključenih u ispitivanje moguće je kontrolirati zadavanjem sljedećih parametrima:

Parametar	Vrijednost	Značenje
bez parametra	-	pregledava se lokalno računalo
/c	<ime_domene>/<ime_racunala>	pregledava se računalo sa zadanim imenom na zadanoj domeni
/i	<xxx.xxx.xxx.xxx>	pregledava se računalo sa zadanom IP adresom
/r	<xxx.xxx.xxx.xxx> - <xxx.xxx.xxx.xxx>	pregledava se zadano područje IP adresa
/d	<ime_domene>	pregledavaju se sva računala na zadanoj domeni

***Tablica 1** - Lista parametara kojima se definiraju ciljna računala*

6.2. Definiranje opsežnosti testiranja

Sljedećim parametrima moguće je precizno definirati koji će se testovi od svih podržanih provoditi. Moguće je zadavanje sljedećih parametara:

Parametar	Vrijednost	Značenje
/n	IIS	isključuje IIS provjere
/n	OS	isključuju se općenite provjere
/n	password	isključuju se provjere zaporki
/n	SQL	isključuju se IIS provjere
/n	hotfix	isključuju se provjere sigurnosnih i *hotfix* zakrpi

***Tablica 2** - Lista parametara kojima se definira opsežnost testova*

6.3. Definiranje izlazne datoteke

Putem naredbenog retka moguće je također zadati lokaciju i ime datoteke u koju će se pohraniti rezultat testiranja.

Parametar	Vrijednost	Značenje
/o	%domain% - %computername% (%date%)	definiranje izlazne datoteke

***Tablica 3** - Lista parametara kojima se definira izlazna datoteka*

6.4. Prikazivanje rezultata testiranja i ostalih detalja

Sljedećim parametrima moguće je utjecati na način prikaza rezultata testiranja.

Parametar	Vrijednost	Značenje
/e	-	ispis grešaka
/l	-	ispis liste svih raspoloživih izvještaja
/ls	-	ispis svih izvještaja posljednjeg testiranja
/lr	<ime_izvjestaja>	ispis kratkog izvještaja testiranja (eng. *overview*)
/ld	<ime_izvjestaja>	ispis detaljnog izvještaja testiranja

***Tablica 4** - Lista parametara kojima se definira prikaz rezultata*

6.4.1. Ostale opcije

Na kraju je dana lista parametar koju je moguće proslijediti programu, a ne spadaju u niti jednu od navedenih skupina.

Parametar	Vrijednost	Značenje
/?	-	pomoć pri korištenju programa
/qp	-	prikaz statusa testiranja
/qe	-	isključivanje ispisa grešaka
/qr	-	isključivanje ispisa liste izvještaja
/q	-	isključivanje svih gore navedenih ispisa (u ovoj tablici)
/f		preusmjeravanje ispisa u zadanu datoteku

***Tablica 5** - Ostali parametri*

7. Zaključak

Provedena testiranja pokazala su da se radi o vrlo ozbiljnom i praktičnom programskom paketu. Program je uspješno detektirao sve ranjivosti deklarirane dokumentacijom, s preciznim opisom i uputama za uklanjanje problema.

Intuitivno i lijepo dizajnirano sučelje olakšava korištenje programa, što je njegova dodatna kvaliteta.

Periodičko pokretanje testova MBSA programom trebao bi biti uobičajeni zadatak svih mrežnih administratora zaduženih za Windows operacijske sustave, budući da se ovim putem može znatno pridonijeti sigurnosti sustava.

Jedini nedostatak primijećen prilikom testiranja je vezan za način pohranjivanja izvještaja. Svi izvještaji trenutno se pohranjuju u čistom tekstualnom obliku (XML format zapisa), što se u određenoj mjeri može smatrati sigurnosnim nedostatkom s obzirom na povjerljive informacije koje izvještaji sadrže.