A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

ALGEBRA

KATEDRA ZA OPERACIJSKE SUSTAVE

Operacijski sustavi

Lab 09 – Sigurnosni mehanizmi

REV 1.0

Sadržaj

Uvod 3
Sigurnosni identifikatori 5
    Sysinternals alati za SID-ove 6
    Pokretanje aplikacija u kontekstu drugog računa 7
Razine integriteta 8
    Protected Mode Internet Explorer 9
Što treba znati nakon ove vježbe? 11

Uvod

Operacijski sustav mora bit u stanju zaštiti vlastite datoteke, memoriju i konfiguracijske postavke od neovlaštenih promjena. Naravno, niti jedna metoda zaštite nije sama po sebi dovoljna, a niti 100% efikasna. Antivirusni alati, *Firewall*, dobro definirana prava pristupa i prvenstveno educirani korisnici su zdrav temelj za siguran sustav. Mi ćemo se u ovoj vježbi koncentrirati na mehanizme koje Windows OS koristi kako bi dao svoj obol sigurnosti. Za početak nabrojimo (ponovimo iz prvog bloka vježbi) osnovne pojmove iz Windows arhitekture vezane za sigurnost OS-a:

- **Security reference monitor** (SRM): komponenta unutar izvršnih servisa Windowsa (implementirana u datoteci **Windows\System32\ntoskrnl.exe**) zadužena za provjeru prava pristupa nad objektom, upravljanjem **korisničkim pravima** (eng. *User rights*) i generiranju poruka s obavijestima vezanima za sigurnost (npr. uspješni ili neuspješni pristup objektu; popularna poruka „Access is denied“).
- **Local Security Authority Subsystem** (Lsass): proces koji radi u korisničkom modu (implementiran u datoteci **Windows\System32\lsass.exe**) zadužen za primjenu i poštivanje sigurnosnih postavki (npr. koji korisnici imaju pravo prijave na računalo, postavke lozinki, prava dodijeljena korisnicima i grupama), autentikaciju korisnika i prosljeđivanje poruka u Event Log datoteku.
- **Lsass baza**: sadrži same sigurnosne postavke lokalnog računala. Baza je pohranjena u Registryju, pod ključem **HKLM\Security**. Sadrži informacije o domenama kojima se vjeruje za autentikaciju prijava korisnika, tko smije pristupiti računalu i kako, ali služi i kao spremnik za **keširane podatke za prijavu** (eng. *Cached credentials*).
- **Security Accounts Manager** (SAM): skup funkcija zaduženih za upravljanje bazom korisnika i grupa definiranih na lokalnom računalu. SAM servis, implementiran kroz datoteku **Windows\System32\samsrv.dll**, izvršava se unutar Lsass procesa.
- **SAM baza**: baza (ne relacijska) koja na računalima koja nisu domenski kontroleri sadrži definicije lokalnih korisnika i grupa, uključujući pripadajuće im lozinke i atribute. Na domenskim kontrolerima SAM sadrži administratorski račun i lozinku za oporavak. SAM baza je pohranjena u Registryju, pod ključem **HKLM\SAM**.
- **Active Directory** (AD): imenički servis (eng. *Directory service*) koji sadrži informacije o objektima unutar domene. Domena je skup objekata (računala, grupa i korisnika) koje se tretiraju kao jedan entitet. Također, u AD se pohranjuju lozinke i prava domenskih korisnika. Te informacije se **repliciraju** na sva računala koja obnašaju ulogu **domenskog kontrolera** (eng. *Domain* controller) domene. AD serverski servis, implementiran u datoteci **Windows\System32\ntdsa.dll**, izvršava se unutar Lsass procesa.
- **Interactive logon manager** (Winlogon): proces koji se izvršava u korisničkom modu, implementiran u datoteci **Windows\System32\Winlogon.exe**. Zadužen je za upravljanje sesijama korisnika koji se interaktivno prijavljuju na sustav. Npr. winlogon kreira korisnikov prvi proces nakon prijave na računalo.
- **Logon user interface** (LogonUI): proces koji se izvršava u korisničkom modu a zadužen je za prikaz korisničkog sučelja putem kojeg se korisnik autenticira računalu. Za dobavljanje korisničkog imena i lozinke koristi **CP** objekte (eng. *Credential providers*), koji su pak implementirani u datoteci Windows\System32\authui.dll.

- **Network logon service** (Netlogon): Windows servis, implementiran u datoteci **Windows\System32netlogon.dll,** zadužen za sigurno povezivanje računala i domenskog kontrolera.

Sigurnosni identifikatori

S obzirom da korisnička imena ne moraju biti jedinstvena, Windowsi koriste **sigurnosne identifikatore** – **SID**-ove (eng. *Security identifiers*) kao jedinstvene identifikatore objekata koji vrše izmjene na sustavu. SID-ovi se dodjeljuju lokalnim i domenskim grupama i korisnicima, računalima, domenama i ostalim članovima domena. SID je, u osnovi, numerička vrijednost varijabilne duljine koja se sastoji od tri dijela:

1. revizijska oznaka SID strukture
2. 48-bitne oznake **autoriteta** koji je izdao SID. Autoritet je lokalno računalo ili domena.
3. 32-bitne oznake **pod autoriteta**, poznatijeg pod oznakom **RID** (eng. *Relative identifier*). RID-ovi se koriste kao „konačna" oznaka objekta kojeg želimo identificirati, a generiraju se nasumično, na osnovu oznake autoriteta.

----------NAPOMENA----------

S obzirom da su SID-ovi vrlo dugi identifikatori, a i Windowsi koriste vrlo napredan generator slučajnih brojeva (puno napredniji od generatora pseudoslučajnih brojeva kojeg ste upoznali u C-u, npr. kroz funkciju *srand()*) za njihovo generiranje, praktički je nemoguć slučaj izdavanja dva identična SID-a. Ova opaska ne vrijedi u slučaju **preslikanih računala** (eng. *Imaged computers*). Na takvim računalima je potrebno resetirati SID-ove pomoću alata **Sysprep** ili **NewSID**.

Svaki SID ima prefiks **S**, dok su tri gore nabrojene komponente odvojene znakom **–** (povlaka), kao u primjeru S-1-5-21-1465213571-1625468621-598698511-1000. Ovdje je oznaka revizije 1, te nakon nje slijede četiri oznake pod autoriteta te jedna oznaka RID-a (1000).

Prilikom instalacije Windowsa, Setup program dodjeljuje računalu i lokalnim korisničkim računima SID. Svaki SID lokalnog računa je baziran na SID-u računala, nakon kojeg slijedi RID. RID-ovi za korisnike i grupe počinju s 1000 i povećavaju se u koracima za 1, za svakog novog korisnika ili grupu.
Dcpromo.exe alat koji se koristi za promoviranje Windows Server sustava u **domenski kontroler** (eng. *Domain controller*) funkcionira na isti način. Dotični alat koristi SID računala koje se promovira u SID nove domene i zatim stvara novi SID za samo računalo. Takvim principom će SID računala ostati jedinstven čak i ako se ono kasnije degradira iz domenskog kontrolera u „običan" server – član domene (eng. *Member server*). Windowsi novim objektima u domeni dodjeljuju SID domene nakon kojeg slijedi jedinstveni RID, koji također počinje s 1000 i povećava se u koracima za 1 za svakog novog korisnika ili grupu. Primjerice, RID s oznakom 1027 označava 28. SID kojeg je domena dodijelila nekom objektu.

----------NAPOMENA----------

Windowsi u određenim slučajevima koriste i fiksne, tj. predefinirane RID-ove. Npr. RID računa **Administrator** je 500, a računa **Guest** je **501**. Dotični RID-ovi su dobro poznati stoga se preporuča da se ti računi **onemoguće** (eng. *Disable*), tj. ne koriste, iz sigurnosnih razloga.

Uz gore navedene SID-ove i RID-ove, valja svakako spomenuti i one dodijeljene grupama korisnika. Npr. SID koji identificira svaki i bilo koji račun (osim anonimnih korisnika) je SID dobro poznate grupe **Everyone**: S 1-1-0. Popis SID-ova za poznate grupe (i scenarij upotrebe) možete vidjeti u tablici 1, preuzetoj iz Windows SDK dokumentacije.
I na kraju, Windowsi generiraju jedinstveni SID za svaku prijavu na sustav, bila ona interaktivna ili ne. Takvi SID-ovi se koriste kroz prava pristupa, tj. **ACE** (eng. *Access control entry*) **zapise**.

SID	Grupa	Upotreba

S-1-0-0	Nobody	Koristi se u slučaju nepoznatog SID-a.
S-1-1-0	Everyone	Grupa uključuje sve korisnike.
S-1-2-0	Local	Korisnici koji su lokalno (fizički) prijavljeni na sustav.
S-1-3-0	Creator Owner	Ovaj SID se zamjenjuje SID-om korisnika koji kreira novi objekt. Koristi se kod nasljeđivanja prava pristupa.
S-1-3-1	Creator Group ID	Ovaj SID se zamjenjuje SID-om primarne grupe korisnika koji je kreirao novi objekt. Koristi se kod nasljeđivanja prava pristupa.
S-1-9-0	Resource Manager	Koriste ga aplikacije koje same vode računa o sigurnosti vlastitih podataka (npr. Microsoft Exchange server).

Tabela 1 Popis SID-ova poznatih grupa

Sysinternals alati za SID-ove

Pomoću alata **PsGetSID** iz Sysinternals grupe se može konvertirati korisničko ime u SID, i obratno. Ukoliko alat pokrenete bez prekidača (argumenata), ispisati će SID dodijeljen lokalnom računalu. U slučaju da je korisnički račun Administrator **preimenovan** (zastarjela sigurnosna praksa, ne preporuča se) korištenjem RID-a 500 možemo vrlo jednostavno saznati novo korisničko ime koje odgovara navedenom računu. Jednostavno ćemo nakon SID-a računala dodati sufiks **-500**, kao u sljedećem primjeru:

1. Preuzmite **PsTools** s linka: https://docs.microsoft.com/en-us/sysinternals/downloads/psgetsid
2. Raspakirajte zip datoteku
3. Pokrenite **Command Prompt** i pozicionirajte se u mapu gdje ste raspakirali PsTools
4. Upišite naredbu **PsGetSid.exe /?**
5. Proučite sintaksu i prekidače PsGetSId naredbe.
6. Upišite naredbu **PsGetSid**. Kojem objektu pripada ispisani SID?
7. SID iz prethodnog koraka upotrijebite kao argument naredbe PsGetSid, sa sufiksom **500**, kao u primjeru:
   psgetsid.exe S-1-5-21-1831018622-1806325766-813394155-500
   Ovdje upišite SID iz prethodnog koraka
   Kojem računu odgovara taj SID?
8. Pronađite SID-ove asocirane s računima:
   a. Guest
   b. Račun s kojim ste trenutno prijavljeni na računalo (hint: ime korisnika možete saznati putem naredbe **whoami**).
9. Zatvorite Command Prompt.

SID-ove možete saznati i pomoću **Process Explorera**. Pratite sljedeće korake:

1. Pokrenite **Process Explorer**
2. Dvostrukim klikom otvorite svojstva bilo kojeg procesa (npr. explorer.exe)
3. Kliknite na karticu **Security**
4. Informacija prikazana u polju **User** sadrži korisničko ime, dok u polju **SID** piše, logično, SID asociran s korisnikom. Provjerite da li ste prethodnu vježbu ispravno odradili.
5. Zatvorite **Process Explorer**.

Pokretanje aplikacija u kontekstu drugog računa

Sigurnosne postavke postavljene na SAM bazu i ključevima s oznakom **Security** u Registryju zabranjuju pristup svim korisničkim računima. Jedina je iznimka račun **Local System**. Drugim riječima, kad bi pokrenuli program **Regedit** i pokušali otvoriti ključ **HKLM\SAM** ostali bi razočarani jer ne bi mogli pregledavati sadržaj, bez obzira što na računalu imate prava lokalnog administratora. Jedan od načina za pristupanje navedenim ključevima, u svrhu njihovog promatranja, jest *reset* dotičnih sigurnosnih postavki. Tom radnjom bi znatno ugrozili stabilnost i sigurnost sustava i nikako to ne radite na „živom" računalu. Kako bi ipak vidjeli sadržaj SAM baze poslužit ćemo se alatom **PsExec** iz Sysinternalsa. Popularnu Windows **RunAs** naredbu ne koristimo jer PsExec alat omogućuje izvršavanje aplikacija (preciznije, izvršnih datoteka) u kontekstu bilo kojeg računa, pa čak i specijalnih kao što je Local System. Pratite sljedeće korake:

1. Pokrenite **Command prompt**
2. Pozicionirajte se u direktorij **PsTools**
3. Upišite naredbu **psexec –s –i –d C:\windows\regedit.exe**
4. Prebacite se na novotvoreni prozor Regedita.
5. Otvorite ključ **HKLM\SAM\SAM\Domains\Builtin\Aliases\Members**
6. Uvjerite se da je na toj lokaciji pohranjen račun lokalnog računala. Kako u to možete biti sigurni?
7. Pod ključem Lokalnog računala provjerite da li se nalazi **SID** Administratora.
8. Zatvorite **Regedit** i **Command prompt**.

Razine integriteta

Ponekad provjera korisnikovog identiteta nije dovoljna za pristup nekom resursu, čak i ako mu prava to dopuštaju. Windowsi koriste **mehanizme za očuvanje integriteta** (eng. *Integrity mechanisms*) kako bi izolirali resurse korisnicima. Dotični mehanizmi su implementirani kroz **UAC** (eng. *User account control*), **PMIE** (eng. *Protected mode Internet Explorer*) i **UIPI** (eng. *User interface privilege Isolation*) komponente Windowsa. Postavlja se pitanje čemu ti mehanizmi? Zašto je potrebno korisniku koji, npr. ima prava lokalnog administratora, onemogućavati pristup u bilo kojem aspektu sustava? Odgovor je, naravno, iz sigurnosnih razloga. Jedan od tipičnih scenarija u kojem se blokira pristup resursima koji bi mogli kompromitirati integritet Windowsa je preuzimanje nepoznate datoteke s Interneta. U tom slučaju će prije spomenuti mehanizmi tražiti potvrdu od korisnika za izvršavanje datoteke, ili mu u potpunosti onemogućiti pristup.

Zaključimo, mehanizmi za očuvanje integriteta mogu nadjačati korisnička prava i prava pristupa, tj. izolirati izvršivi kod i podatke unutar korisničkog konteksta. Kao sustav klasifikacije rizika koji određena datoteka predstavlja koriste se **razine integriteta** (eng. *Integrity levels*), koje se, pak, označavaju SID-ovima, kao što prikazuje donja tablica.

SID	Ime (razina)	Opis
S-1-16-0x0	Untrusted (0)	Koriste ju procesi pokrenuti iz grupe **Anonymus**. Uglavnom se blokiraju svi zahtjevi za pisanje po disku ili memoriji.
S-1-16-0x1000	Low (1)	Koristi ga Internet Explorer u Protected Mode načinu rada. Blokiraju se zahtjevi za pisanje na većinu objekata, npr. na datoteke i u Registry.
S-1-16-0x2000	Medium (2)	Koriste ga „normalne“ aplikacije prilikom pokretanja uz uključeni UAC
S-1-16-0x3000	High (3)	Koriste ga aplikacije pokrenute s administratorskim pravima uz uključeni UAC, ali i aplikacije pokrenute dok je UAC isključen a aktivni korisnik je lokalni administrator.
S-1-16-0x4000	System (4)	Koriste ga servisi i sistemske aplikacije (npr. Wininit, Winlogon…)

Tabela 2 Razine integriteta

Pomoću Process Explorera možete vidjeti razinu integriteta za svaki proces pokrenut na sustavu, kao što prikazuje sljedeći primjer:

1. Kliknite na **Start** gumb i upišite **UAC**
2. Kliknite na opciju **Change User Account Control settings**
3. Vrijednost klizača postavite na 3. vrijednost: **Default – Notify me only when programs try to make changes to my computer**
4. Kliknite na gumb **OK**.
5. Pokrenite **Internet Explorer**
6. Pokrenite **Command Prompt** kao administrator (**desni klik** na ikonu Command Prompta, opcija **Run as Administrator**).
7. Pokrenite **Paint**.
8. Pokrenite **Process Explorer**.
9. Kliknite na **View->Select Columns**, označite opciju **Integrity Level** i kliknite na gumb **OK**.

10. Kliknite na **File->Show Details for All Processes**.
11. Provjerite da su razine integriteta Internet Explorera, Painta i Command Prompta postavljene, redom, na **Low**, **Medium** i **High**. Primijetite da su sistemski procesi i servisi označeni s najvišom oznakom, **System**. Ukoliko ne vidite sistemske procese (npr. Lsass.exe) kliknite na **View->Show Processes from all Users**.
12. Zatvorite **Process Explorer** i sve ostale pokrenute programe.

Oznake integriteta se dodjeljuju i drugim objektima uz procese, kao što su datoteke i ključevi u Registryju. Njihove oznake možete vidjeti pomoću alata **Accesschk** iz Sysinternals grupe, kao što prikazuje sljedeći primjer:

1. S internet preuzmite AccessChk aplikaciju s linka: https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk
2. Raspakirajte je.
3. Pokrenite Command Prompt kao administrator (**desni klik** na ikonu Command Prompta, opcija **Run as Administrator**).
4. Pozicionirajte se u direktorij gdje ste raspakirali **AccessChk**
5. Upišite naredbu **accesschk –e C:\Users\admin\AppData** (umjesto **admin** upišite naziv vašeg korisničke mape koja se nalazi u **Users** mapi na sistemskom disku)
6. S obzirom da smo upotrijebili prekidač **–e**, naredba je ispisala samo eksplicitno postavljene oznake integriteta.
7. Zatvorite **Command Prompt**.

Principi nasljeđivanja su duboko ugrađeni u brojna područja Windowsa (NTFS prava pristupa, AD…), pa tako i u oznake integriteta. Njihova pravila su:

- Proces dijete nasljeđuje razinu integriteta od svog roditelja. Npr. Command Prompt pokrenut s administratorskim ovlastima će također pokretati nove procese unutar administratorskog konteksta, tj. s oznakom integriteta High.
- U slučaju konflikata prilikom dodjele razine integriteta, vrijedi pravilo manje privilegije. Drugim riječima, ukoliko su u mogućnosti birati, Windowsi dodjeljuju nižu oznaku integriteta (ne zaboravimo, niža oznaka znači „sigurnije“ korištenje procesa).
- Proces roditelj može stvoriti proces dijete s eksplicitno postavljenom vrijednošću integriteta. Npr. ukoliko iz Command Prompta pokrenutog s administratorskim ovlastima pokrenete Internet Explorer u *Protected Modeu*, dotični će imati oznaku *Low*. Ovo pravilo je iznimka prvog pravila.

Protected Mode Internet Explorer

Protected Mode Internet Explorer (**PMIE**) je način rada web preglednika predstavljen s verzijom 7 Internet Explorera. Zadaća mu je iskoristiti ugrađene sigurnosne mehanizme Windowsa kako bi zaštitio računalo i korisnika od potencijalnih prijetnji s Interneta. Za demonstraciju PMIE-a poslužit ćemo se Proces Monitorom:

1. Pokrenite **Process Monitor**
2. Ukoliko se odmah ne prikaže dijalog za konfiguraciju filtra kliknite na izbornik **Filter->Filter**. Zatim iz filtarskog dijaloga postavite sljedeće parametre:
    a. Prvi padajući izbornik: **Proces Name**
    b. Drugi padajući izbornik: **Is**

   c. Okvir za unos teksta: **iexplore.exe**
   d. Treći padajući izbornik: **Include**
   e. Kliknite na gumb **Add** i zatim na **OK**.
3. Ne zatvarajući Process Monitor, pokrenite **Process Explorer**.
4. Kliknite na **View->Select Columns**, označite opciju **Integrity Level** i kliknite na gumb **OK**.
5. Sad pokrenite Internet Explorer. Nakon što se pokrene, Process Explorer će prikazati dva nova procesa **iexplore.exe** s oznakom integriteta Low i Medium. Upravo ovdje se vidi implementacija **PMIE** mehanizma – dva procesa, koji su, zapravo, različite komponente preglednika, s različitim oznakama integriteta.
6. Prebacite se na Process Monitor i isključite prikaz događaja iz Registryja, mreže i s datotečnog sustava (gumbi na alatnoj traci **Show Registry Activity, Show Network Activity** i **Show File System Activity**). Također, desnim gumbom miša kliknite na bilo koji događaj s oznakom **Load Image** u stupcu **Operation** i iz kontekstualnog izbornika odaberite opciju „**Exclude Load Image**“. Ovim radnjama smo broj zapisa u Process Monitoru sveli na razinu prihvatljivu za analizu.
7. Dvostrukim klikom otvorite svojstva (eng. *Properties*) događaja (eng. *Event*) s oznakom **Process Start** (prvi prikazani događaj) i kliknite na karticu **Process**. Koji je integritet tog prvog procesa?
8. Kliknite na gumb **Close.**
9. Dvostrukim klikom otvorite svojstva idućeg događaja s oznakom **Process Start** i kliknite na karticu **Process**. Koji je integritet tog procesa?
10. **Zatvorite** Internet Explorer. Process Monitor će zabilježiti nove događaje povezane s prekidanjem izvođenja procesa Internet Explorera.
11. Otkrijte kojim redoslijedom su se isključivali procesi:
    a. Da li je prvi isključen proces s oznakom Medium ili Low?
    b. Da li je vaš pronalazak u suglasju s pravilima o nasljeđivanju integriteta procesa?
12. Zatvorite **Process Monitor** i **Process Explorer**.

Što treba znati nakon ove vježbe?

1. Definirati SRM
2. Definirati Lsass
3. Definirati SAM
4. Objasniti ulogu i strukturu SID-a
5. Objasniti zašto je potrebno onemogućiti račun Administrator
6. Objasniti čemu služe razine integriteta
7. Nabrojati razine integriteta
8. Objasniti nasljeđivanje razina integriteta