Virtualios infrastruktūros sauga

VI diegimo ir valdymo sauga

Diegimas ir valdymas

VI diegimas ir valdymas iššaukia saugumo grėsmes dėl vykdomų komunikacijų tarp:

- VIC ir VC
- VIC ir ESX
- WebAccess ir ESX
- VDM ir ESX, VC
- CLI ir ESX
- Remote CLI ir ESX

Grėsmės siejamos su: tapatybės valdymu (autorizacija, autentifikacija, rolės, teisės), prieigos ribojimais.

Duomenų srautai

- Visi duomenų srautai tarp minėtų įrenginių yra šifruoti naudojant SSL.
- VMware naudoja savo paties pasirašytus sertifikatus (self-signed).
- SSL viena iš saugos grėsmių Man-in-the-Middle injekcija.

- SSL naudoja 443 portą
- ESX naudoja reversinį proxy, kuris slepia gavėjo porto numerį nuo kliento ir tokiu būdu sumažina atakos tikimybę.

VIC ir VC

VIC – VC komunikuoja per 80 portą, persijungia į 443 inicializacijai ir toliau dirba 902 portu.

VC ir ESX srautas eina per SSL tunelį 902 portu, nors inicializacija vykdoma per 443 portą.

Grėsmės:

- SSL atakos galimos tarp VC ir ESX per 902 portą
- SSL atakos galimos tarp VIC ir VC per 443 portą
- SSL atakos galimos tarp VIC ir ESX per 902 portą

VIC ir VC

VIC ir VC grėsmių valdymas:

- Apibrėžti VIC vartotojo teises VC:
  - Monitoringas
  - Atnaujimimų valdymas
  - VM valdymas
  - VM diegimas
- Naudojant daugelį VC infrastruktūrai valdyti, apibrėžiamos atitinkamos teisės į kiekvienos VI valdymo paslaugas.

VIC ir VC tapatybės valdymas

Vartotojai, apibrėžti VC, naudojami prisijungimui. VC nepalaiko dvigubos autenifikacijos, t.y. prisijungimas prie darbo vietos nesuteikia prisijungimo prie VC.

VC taip pat nepalaiko SSO, kuris bendruoju atveju turi saugumo grėsmių.

VC ir ESX tapatybių valdymas gali būti integruotas su AD, eDirectory, LDAP, NIS.

VC ir WebAccess

Prisijungimo prie VC per WebAccess procesas:

- Pirma užklausa įvykdoma per 80 portą;
- Naudojamas reversinis proxy per 8009 portą, per kurį sudaromas SSL tunelis.

Prisijungimo prie ESX per WebAccess procesas:

- Pirma užklausa įvykdoma per 80 portą;
- Persijungiama į 443 portą, per kurį sudaromas SSL tunelis.

SSH į ESX

- Pagal nutylėjimą draudžiamas prisijungimas per SSH root vartotojui
- SSH dirba per 22 portą. Porto numeris gali būti keičiamas.
- Atidarius SSH portą, reikia drausti prisijungimą root vartotojui
- SSH naudoja „preshared“ raktus, todėl galimas SSO

Prisijungimas prie konsolės

Daugelis serverių gamintojų palaiko nuotolinį prisijungimą prie serverio konsolės, pavyzdžiui:

- HP Integrated Lights Out (ILO)
- Dell Remote Access Card (DRAC)

Tam paprastai sudaromas atskiras tinklas.

Prisijungimas vykdomas per 80 portą, permetant į 443.

Atnaujinimų valdymas

- Atnaujinimų valdymas atliekamas tiesiogiai jungiantis į Vmware Patch repository wmware.com svetainėje. Prisijungimas per 80 portą, po to permetama į 8084.
- Atnaujinimų menedžeris atsisiunčia atnaujinimus ir juos pasideda į lokalų repozitoriumą.
- Atnaujinimus valdo procesas *esxupdate*.

Tapatybės valdymas

- Autentifikacija ir autorizacija
- Split-Brain autentifikacija – kai infrastruktūroje taikomi daugiau nei vienas būdas vartotojų autentifikavimui.
  - VC – administrator
  - ESX – root

- Turi būti sąsaja (maping) tarp skirtingų vartotojų. Tai kartais gali sukelti problemų, kai naudojamos direktorijų tarnybos.
  - Pvz. Persikrovimo metu, nepasiekiant AD serverio negalima prisijungti prie ESX, nes vartotojo duomenys (credentials) Linux sistemoje priešingai nei Windows nesikešuoja.

Tapatybės valdymas

Saugumo rekomendacijos:

- Tik root vartotojas gali turėti tiesioginį prisijungimą prie ESX naudojant VIC
- Tik administratoriaus teises turintys vartotojai gali prisijungti prie VC per VIC. Kiekvienam administratoriui turi būti apibrėžtos rolės ir suteiktos atitinkamos teisės.
- Turėtų būti naudojama skirtinga vartotojų autorizacija VC ir ESX.
- Apibrėžti konkrečias roles vartotojams
- Sujungti visas vartotojui priskirtas roles skirtingose tapatybės valdymo sistemose

Tapatybės valdymas

Saugumo rekomendacijos:

- Visus nekritinius vartotojus prijungti prie VI per direktorijų tarnybą
- Įjungti nuotolinį įvykių registravimą į centralizuotą įvykių registrų žurnalą
- Periodiškai audituoti įvykių žurnalą, atkreipiant dėmesį į autentifikaicjos ir autorizacijos įrašus.
- Kai naudojama tapatybės valdymo sistema, apriboti lokalius ESX vartotojus
- Žurnalo failai turi ataskyti į klausimus kas, kada, iš kur, kaip.
- Žurnalo failai turi pateikti pakankamai informacijos, kad galima būtų pradubliuoti įvykį.

Nuotolinis žurnalas

- Windows OS neturi galimybės vesti nuotolinio įvykių žurnalo, todėl reikia naudoti papildomas priemones. Pvz. Snare.
- Atkreipti dėmesį, kad VC įvykiai registruojami kataloge:
- C:\.....\Vmware\Vmware VirtualCenter\Logs
- ESX konfigūruojamas kaip Linux t.y. konfigūraciniame faile /etc/syslog.conf
- ESX įvykių žurnalai saugomi /var/log/ kataloguose.
- ESXi konfigūruojant galima naudoti RCLI komandą *vicfg-syslog*

Direktorijų tarnyba

VMware ESX palaiko tokias direkorijų tarnybas:

- LDAP, LDAP-S
- Novell eDirectory
- Microsoft AD
- NIS

ESXi iki 5.0 nepalaikė direktorijų tarnybos, kaip nemokamas produktas, neskirtas komerciniam naudojimui.

Sertifikatai

Visuose prisijungimuose prie ESX ar VC naudojamas SSL tunelis.

Grėsmė – MiTM ataka, kai naudojamas blogas sertifikatas.

Instaliuojant SSL, reikalingas sertifikatas, kuris patvirtintų serverio tapatybę.

Jei įmonė neturi sertifikato, išduoto žinomos šaknинės sertifikavimo tarnybos CA (pvz. GlobalSign, CAcert.org, Comodo, Verisign ir t.t.), tuomet serveris susikuria savo sertifikatą, kuriuo turėtų pasitikėti vartotojas.

Sertifikatai tikrinami žmogaus arba programiškai.

Sertifikatai

Sertifikato vienas iš komponentų – privatus raktas, kuris yra PKI infrastruktūros dalis.

Privatus serverio raktas sudaromas pagal X.509 standartą, šifruojamas pagal *base64* schemą ir fiziškai tai failas, turintis pem plėtinį.

Žinomų CA sertifikatai yra patikimi.

VMware naudoja savo pasirašytus sertifikatus.

Sertifikatų failai gali būti keičiami tiek VC, tiek ir ESX pusėje (rui.crt ir rui.key).

Diegimo ir valdymo tinklo sauga

Rekomendacijos didinant tinklo saugą:

- VC ir ESX turi būti už ugniasienės
- Naudoti IPsec tarp VIC ir VC
- Naudoti VPN arba SSH tunelius

Diegimo serveriai

P2V diegimas naudojamas virtualioje infrastruktūroje.

Tai susiję su tokiomis grėsmėmis:

- Perėjimas į skirtingas saugumo zonas
- Įrenginių pasiekimas gali būti ribojamas (USB, FireWire, eSATA)
- Skirtinga tinklo konfigūracija; DHCP, DNS
- Neteisingas duomenų saugykla
- Virusai ir kirminai iš fizinės mašinos gali būti pernešami į VM tinklą.
- Pirmas VM (buvusios fizinės mašinos) paleidimas turi būti saugioje aplinkoje (sandbox)
- Įmonė privalo turėti procesą, skirtą VM kūrimui, diegimui, trinimui.

Apibendrinimai

- Diegimo ir valdymo funkcijos intensyviai naudoja komunikacijas.
- VIC -> VC, ESX naudoja SSL ir reversinį proxy
- Katalogų tarnybos naudojamos VI
- Centralizuotas žurnalinių įrašų saugojimas
- P2V diegimas