Virtualios infrastruktūros sauga

Virtualios infrastruktūros saugos stiprinimas (hardening)

Saugos stiprinimo kryptys

Virtualios infrastruktūros hypervizorių saugos stiprinimo kryptys:

- Hypervizoriaus valdymo konsolė (vartai į VI)
- Virtualios mašinos
- Tinklo apsaugos stiprinimas
- Auditavimo galimybių didinimas (leidžia pasakyti, kas, kur ir kada įvyko)
- Monitoringo stiprinimas (stebėjimas realiu laiku)
- Pasiruošimas elektroninio nusikaltimo tyrimams

Saugos stiprinimas

Hypervizorių gamintojai išleidžia rekomendacijas (gerąsias praktikas), skirtas sistemų administratoriams ir saugos specialistams (pvz. CISO).

VMware

http://www.vmware.com/support/support-resources/hardening-guides.html

Microsoft

http://technet.microsoft.com/en-us/library/dd569113.aspx

Citrix XenServer

http://www.ptsecurity.com/download/XenServer-Free-5-6-SHG.pdf

Saugos stiprinimas

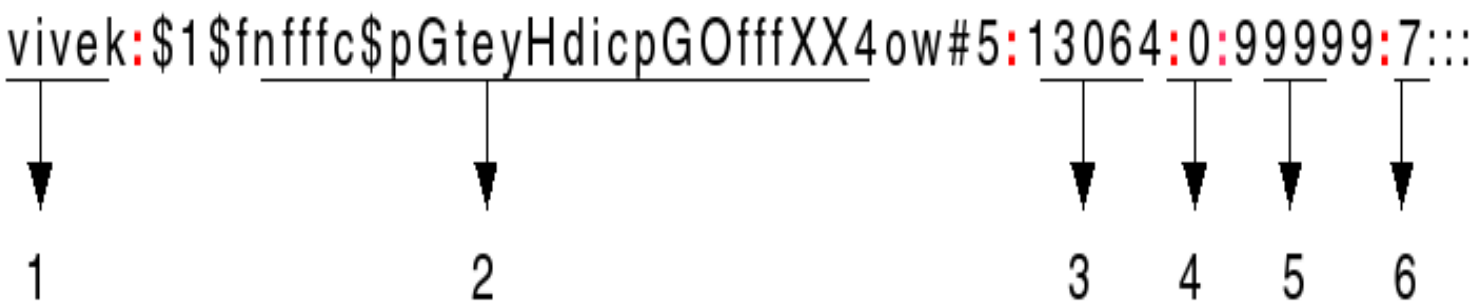
Hypervizoriaus valdymo konsolė, serviso konsolė

- Riboti vartotojų skaičių, kuriems leistina prisijungti tiesiogiai prie konsolės arba naudojant VIC.
- Riboti kompiuterių skaičių, iš kurių leistina prisijungti.
- Administratoriams turi būti suteikiamas atitinkamos rolės, jų užduotims atlikti su atitinkamomis teisėmis (RBAC, pvz. backup administrator)
- Atjungti nenaudojamus virtualius įrenginius, ypač skirtus išorinėms laikmenoms skaityti.

root prisijungimo stiprinimas

- root vartotojo slaptažodis turi būti žinomas tik keliems žmonėms, bet mažiausiai 2.
- Prisijungimas prie hypervizoriaus valdymo konsolės root vartotojui neturi būti leidžiamas (Lockdown mode – enable).
- Prisijungimui naudoti lokalius (arba iš direktorijų tarnybos pvz. AD) vartotojus ir su komanda `sudo` vykdyti komandas root teisėmis. Konfigūruojama `/etc/sudoers` faile.
- Šešėliniai (shadow) slaptažodžiai turi būti įjungti (tai padaryta pagal nutylėjimą, bet reikia pasitikrinti). Slaptažodžiai saugomi šifruoti `/etc/shadow` faile.
- Neleisti prisijungimo prie valdymo konsolės per SSH.

/etc/shadow



1 – prisijungimo vardas (username)

2 – šifruotas slaptažodis. Min. 6-8 simboliai + specialūs simboliai/skaičiai

3 - slaptažodžio paskutinio keitimo data (lastchanged): dienos nuo Jan 1, 1970

4 - min dienų skaičius tarp slaptažodžio keitimų (keitimo dažnis)

5 - dienų skaičius, kurį dar galioja slaptažodis

6 - Dienų skaičius, po kurio vartotojas gaus pranešimą, kad jos slaptažodis galiojimas baigiasi

7 – Dienų skaičius, rodantis, kiek laiko praėjo nuo slaptažodžio galiojimo pabaigos

ESX CLI komanda: `esx-cfg -auth –enableshadow`

Saugos stiprinimas

Pateikiami bendrieji ESXi serverio saugos stiprinimo rekomendacijos.

- Hypervizorius turi veikti saugioje tinklo zonoje t.y. ne DMZ zonoje, o už ugniasienės (patartina naudoti perimetro apsaugos įrenginius UTS - **Unified threat management** įrenginius).
- Naudoti nuotolines žurnalinių įrašų saugyklas, patartina centralizuoti serverių žurnalinių įrašų saugojimą.
  - Įsilaužimo į hypervizorių atveju, žurnalai nepasiekiami
  - Galima atlikti **įrašų koreliacijos analizę**, siekiant išsiaiškinti grėsmes ar atlikti nusikaltimo tyrimą.

Koreliacija

Koreliacija (arba **koreliacijos koeficientas**) tikimybių teorijoje ir statistikoje yra statistinis ryšys tarp kintamųjų.

Koreliacijos koeficientas – tai koreliacijos stiprumo matas. Jeigu dviejų kintamųjų koreliacijos koeficientas lygus nuliui, tai tie kintamieji yra statistiškai nepriklausomi.

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \cdot \sum_{i=1}^{n}(y_i - \bar{y})^2}}$$

Koreliacijos koeficiento reikšmių skalė

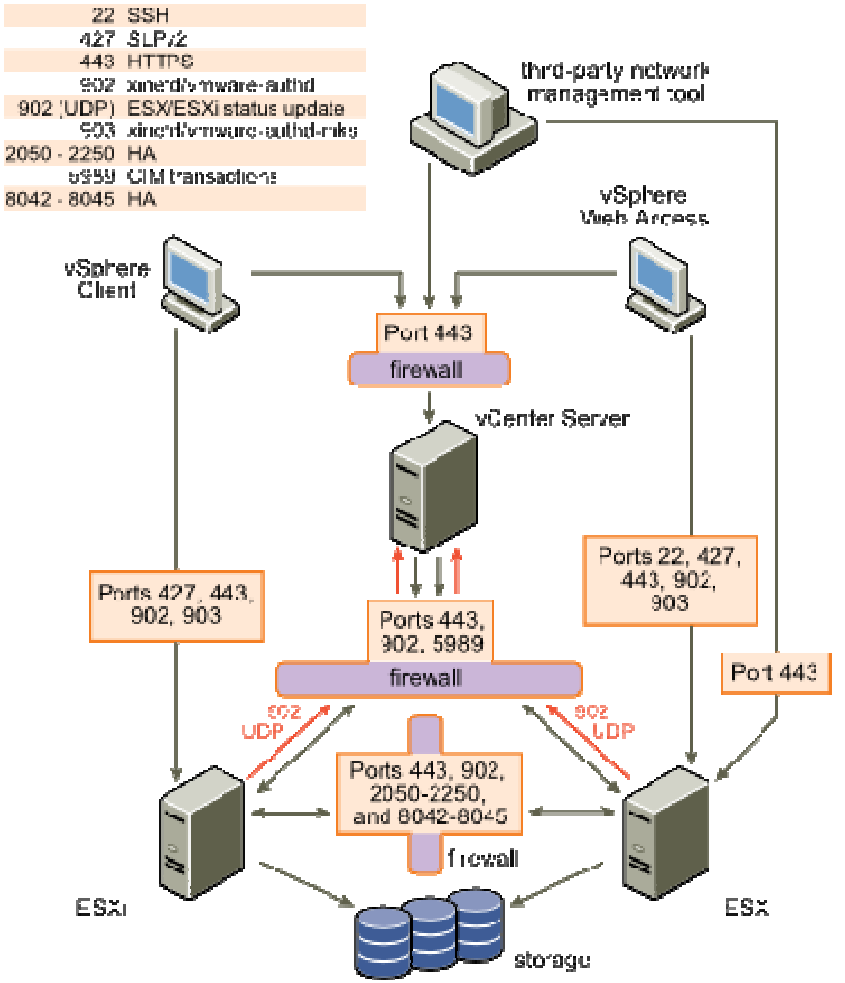
Labai stipri	Stipri	Vidutinė	Silpna	Labai silpna	Nėra ryšio	Labai silpna	Silpna	Vidutinė	Stipri	Labai stipri
-1	nuo -1 iki -0,7	nuo -0,7 iki -0,5	nuo -0,5 iki -0,2	nuo -0,2 iki 0	0	nuo 0 iki 0,2	nuo 0,2 iki 0,5	nuo 0,5 iki 0,7	nuo 0,7 iki 1	+1

Saugos stiprinimas

- Būtinas periodinis atnaujinimų instaliavimas, patartina naudoti vSphere Update Manager.
- Atnaujinimai turi būti siunčiami iš VMware serverių.
- Hypervizorius turi būti apsaugotas vidine ugniasiene.

```
esxcfg-firewall
esxcli network firewall
```

- (*nepatartina naudoti Linux komandų, kurios dar veikia senesniuose ESX*)



Saugos stiprinimas

IP ir portų filtravimas

- Naudoti SNMP protokolą monitoringo sistemoms tik esant poreikiui (pagal nutylėjimas SNMP išjungtas). Ugniasienėje atidaryti prievadą 161, 162 tik monitoringo serveriui.
- Leisti prisijungti prie serviso konsolės, VC tik iš tam tikrų IP adresų.
- Leisti prisijungti per 22 (ssh) ir 59xx (vnc) tik atitinkamiems vartotojams iš tam tikrų IP adresų.
- Naudojant iSCSI saugyklas leisti naudotis prievadu 3260 tik saugyklų IP.

Konfigūravimui naudoti ESX ugniasienę arba TCP Wrapper
(/etc/hosts.allow ir /etc/hosts.deny)

Saugos auditavimas

Rekomenduojama prieš suteikiant serveriui „*production*“ statusą, atlikti jo saugos patikrą.

Patikros įrankiai:

- CIS-CAT https://benchmarks.cisecurity.org/downloads/audit-tools/
- Bastille http://www.bastille-linux.org/
- Tripwire ConfigCheck (ESX 3.x) http://www.vmware.com/support/support-resources/configcheck.html

Auditavimas, skenavimas (pvz. NMAP) ir rezultatų analizė turi būti periodiniai.

CIS-CAT

CIS-CAT tai saugos nustatymų skenavimo įrankis, parašytas Java, skirtas Linux sistemų saugos patikrai (RHEL).

Veikia komandiniame režime ir grafiniame lange.

Vertina kiekvieno testo rezultatus procentais.

Checklist

⊠	A	W	Benchmark Item	Result
1 Patches and Additional Software				
F	+	1.0	1.1 Apply latest OS patches	fail
?	+		1.2 Validate your system before making changes	notchecked
F	+	1.0	1.3 Configure SSH	fail
F	+	1.0	1.4 Install TCP wrappers package	fail
2 Minimize inetd network services				
F	+	1.0	2.1 Disable standard Services	fail
F	+	1.0	2.2 Configure TCP wrappers to limit access	fail
P	+	1.0	2.3 Only enable telnet if absolutely necessary	pass
P	+	1.0	2.4 Only enable FTP if absolutely necessary	pass
P	+	1.0	2.5 Only enable rlogin/rsh/rcp if absolutely necessary	pass
P	+	1.0	2.6 Only enable TFTP Server if absolutely necessary	pass
P	+	1.0	2.7 Only enable Kerberos-related daemons if absolutely necessary	pass
P	+	1.0	2.8 Only enable rquotad if absolutely necessary	pass
P	+	1.0	2.9 Only enable CDE-related daemons if absolutely necessary	pass
3 Minimize Daemon Services				
F	+	1.0	3.1 Disable login prompts on serial ports	fail
P	+	1.0	3.2 Disable inetd, if possible	pass
F	+	1.0	3.3 Disable email server, if possible	fail
F	+	1.0	3.4 Disable NIS Server processes if possible	fail

Bastille

„Bastille” programa skirta operacinės sistemos saugumo stiprinimo rekomendacijų pateikimui. Bastille gali įvertinti esamą sistemos konfigūracijos saugumo lygį, pateikti išsamią ataskaitą.

http://www.bastille-linux.org/

Palaiko Red Hat (Fedora Core, Enterprise), SUSE, Debian, Gentoo, Mandrake distribucijas, taip pat HP-UX.

Failų teisės

Siekiant padidinti prieigos prie failų saugumą, rekomenduojama pasikeisti standartinę teisių kaukę iš 027 į 077 kuriant failus.

Demon‘ams palikti kaukę 027.

Įvykdžius šį reikalavimą, būtų:

Failai rwx - - - - - - root root

Demonai rwx r - x - - - root root

Svarbu! Serveryje neturi būti failų su rašymo galimybe „kitiems (other)“ vartotojams.

Saugos stiprinimas

Niekada nereikia hypervizoriui priskirti papildomų funkcijų (pvz. failų serveris, spausdinimo serveris, DNS ar SQL serveris).

Tvarkaraščių komandomis (`cron` ir `at`) gali naudotis tik root vartotojas.

`chmod, shutdown` komandomis gali naudotis tik root vartotojas.

Pakeisti teises į 600 `/etc/inittab`, kad eiliniai vartotojai nematytų, kaip vykdoma serverio krovimosi eiga.

Saugos stiprinimas

Siekiant atlikti nusikaltimo tyrimą, reikia nustatyti NTP serverį. Nustatymai atliekami `/etc/ntp.conf` faile arba per VIC.

ESX serviso konsolei yra siūlomos antivirusinės programos (Symantec, McAfee, F-Secure). Negalima skenuoti katalogo /vmfs (pagal nutylėjimą taip ir nustatyta), dėl galimai didelio apkrovimo VM.

Žurnaliniai įrašai turi būti saugomi pakankamai ilgą laiką, siekiant juos audituoti, įvykus saugumo incidentui ar elektroniniam nusikaltimui.

NTP protokolas

Network Time Protocol (NTP) – tai tinklo protokolas, naudojamas kompiuterių laikrodžių sinchronizavimui.

NTP naudoja **Coordinated Universal Time** (UTC) kompiuterių laikrodžių sinchronizavimui milisekundžių tikslumu.

NTP protokolas naudojamas nuo 1985 m. ir yra vienas seniausių inerneto protokolų. Naudojamas UDP protokolas, dirba 123 portu.

NTP autorius prof. David Mills (Delaware universitetas).

NTP protokolas

NTP sinchronizuoja visus kompiuterius kelių milisekundžių tikslumu su **Coordinated Universal Time** (UTC). Kompiuterio laikrodžio tikslumas priklauso nuo tinklo pralaidumo.

Praktiškai LAN tinkle tikslumas būna iki 1ms, globaliame tinkle dešimtys milisekundžių.

Veikimo principas

NTP dirba kliento serveriu rėžimu. Klientas siunčia užklausą apie laiką, serveris atsako. Prieš nustatant laiką apskaičiuojamas round-trip delay, kuris pridedamas prie iš serverio gauto laiko.

Užklausos siunčiamas vidutiniškai kas 10 min.

NTP

2010 m. patvirtintas NTP v4, kuris aprašytas RFC 5905.

Versija 4 suderinta su versija 3, kuri aprašyta RFC 1305.

NTP naudoja UDP ir palaiko transliacinį sinchronizacijos tipą.

NTP gali būti panaudojamas DoS atakoms, nes serveris atsakinėja į neautorizuotas užklausas (*spoofed IP*), ir siunčia didelius paketus į mažas užklausas.

NTP protokolas

- NTP naudoja hierachinę, sluoksninę laiko šaltinių (serverių) sistemą. Kiekvienas hierarchijos lygmuo vadinamas **stratum** ir pradedamas numeruoti nuo 0.
- Lygmens numeris rodo, laiko serverio atstumą nuo pagrindinio laiką skaičiuojančio serverio.
- **Stratum 0** – tai aukščiausio tikslumo laiko matavimo įrenginiai:
  - atominiai laikrodžiai
  - GPS,
  - Radio laikrodžiai
- Jie generuoja labai tikslų impulsų skaičių per sekundę, kuris ir panaudojamas laikui skaičiuoti.

NTP protokolas

- **Stratum 1** – tai kompiuteriai, kurie sinchronizuoja savo laiką su Stratum 0 įrenginiais kelių mikro-sekundžių tikslumu. Šie serveriai gali sinchronizuotis tarpusavyje. Jie dar laikomi pirminiais laiko serveriais.
- **Stratum 2** – tai kompiuteriai, kurie sinchronizuoja savo laiką su Stratum 1 įrenginiais. Paprastai sinchonizacija vykdoma su keliais Stratum 1 serveriais ir tarpusavyje.
- Kiti Stratum lygmenys veikia analogiškai, kaip aprašyta ankščiau. Didžiausias stratum lygmuo yra 15.

Algoritmas

NTP klientas nustatydamas tikslų laiką, apklausia 3 ar daugiau serverių. Norint sinchronizuoti laiką su nuotoliniu serveriu, reikia apskaičiuoti *round-trip* laiką ir nuokrypį (*offset*).

Round-trip uždelsimas δ randamas taip:

$$\delta = (t_3 - t_0) - (t_2 - t_1)$$

t_0 – kliento laiko atžyma, rodanti užklausos paketo išsiuntimo pradžią,

t_1 - serverio laiko atžyma, rodanti užklausos paketo priėmimą

t_2 - serverio laiko atžyma, rodanti paketo išsiuntimo laiką

t_3 – kliento laiko atžyma, rodanti paketo gavimo laiką

Algoritmas

Laiko nuokrypis randamas taip:

$$\theta = \frac{(t_1 - t_0) + (t_2 - t_3)}{2}$$

Apskaičiuoti dydžai δ ir θ yra filtruojami bei statistiškai apdorojami. Apskaičiuojamas jų vidutinės reikšmės ir nustatomas kompiuterio laikrodis.

Toks laiko nuokrypio apskaičiavimo būdas teisingas, jei tinklas yra **simetriškas** t.y. keliai pirmyn ir atgal sutampa ir turi tą patį uždelsimą.

Jei tinklas **nesimetrinis**, tuomet apskaičiuojamas sisteminis nuokrypis, kuris lygus pusei laiko gauto atėmus siuntimo pirmyn ir atgal laikus.