25. Tõrkeotsing

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 25. Tõrkeotsing
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.40

Sisukord

25.1. Sissejuhatus

Selles õppetükis antakse juhiseid turvaserveris esineda võivate probleemide lahendamise kohta. Sulle antakse kontroll-loend juhistega kõige sagedamini esinevate probleemide põhjuste leidmiseks. Pärast õppetüki läbimist oskad sa tõrkeotsinguks kontrollida süsteemilogisid ning uurida probleeme järgmiste tööriistadega: tcdump, strace ja Isof.

Õppetüki läbimiseks kulub aega umbes 15 minutit.

25.2. Kontroll-loend

Kui te avastate, et teie turvaserver ei tööta õigesti, vaadake läbi järgmine kontroll-loend.

Kontrolli töövõimeaega.
Kui server on just taaskäivitunud, on võimalik, et peate allkirjastamissertifikaadi kasutamiseks sisestama PIN-koodi.

Kontrolli teenuseid.
Kui server on just taaskäivitatud, ei pruugi kõik teenused veel töötada. Vastasel juhul vaata üle kõik põhitoimingud ja kontrolli, kas need töötavad.

Kontrolli kettaruumi.
Üks sagedamini esinevaid põhjusi teenuse seiskumisel on tööruumi otsasaamine kõvakettal.

Kontrolli koormust.
Kontrolli, kas turvaserveri koormus on tavaline. Kui see on juba enam kui 400% saadaolevast CPU-mahutavusest tipptundidel, on teil uurimist vajav probleem. Põhjuseks võib olla see, et sõnumi suurus võib põhjustada java kokkujooksmise või turvaserverite keskmine teenuste tarbimine nõuab rohkem ressursse.

Kontrolli võrgundust.
Pingi igat hosti avalikus Internetis, mis peaks olema saadaval. Pingi kohalikku infosüsteemi. Kontrolli Telneti abil teenusepordi saadavust (kohalikust võrgust näiteks: `telnet <security server ip> 80`). Kontrolli, kas nimeserverid on saadaval ja töötavad korralikult ja testi samamoodi hostinime, et näha, kas nime resolvimine töötab õigesti.

Käita ping iga eeldatavalt töötava hosti kohta.
Võib-olla on võrgukabel lihtsalt lahti tulnud. Kasutage Telnetti, et kontrollida, kas teenusepordi liiklus on avatud.

Kontrolli kellaaega.
Turvaserver peab olema ühendatud võrguaja protokolli (NTP) 1. või 2. kihi ajaserveriga. Kas need nõuded on täidetud ja kui palju erineb aeg reaalajast?

Kui serveris on võrgu failisüsteemi (NFS) ühendus näiteks logimise või varundamise jaoks, siis kontrolli ühendatud kettaid.
Kontrolli, kas ressurss on veel saadaval.

Paljude nende kontrollide vältimiseks leia aega ja installi monitooring (vt siit).

25.3. Süsteemilogide kontrollimine

Kui ükski eeltoodud lahendus ei aidanud, võib kasulikku teavet leida turvaserveri süsteemilogidest.

Vaata viimaseid sisestusi asukohas:

```
sudo tail –f /var/log/
syslog
```

```
sudo tail –f /var/log/
auth.log
```

Teenuseoleku kontrollimiseks tee järgmist.

```
sudo service xroad-con
fclient status
```

Kõigi X-tee teenuste korraga kontrollimiseks (v.a `nginx`) tee järgmist.

```
sudo initctl list | gr
ep "^xroad-"
```

Teenuse taaskäivitamiseks ja selle logi jälitamiseks tee järgmist.

```
sudo service xroad-jet
ty restart;sudo tail -
f /var/log/xroad/jett
y/jetty.log
```

Turvaserveri kõige olulisemaid süsteemiteenuseid tutvustati siin.

25.4. Probleemide uurimise tööriistad

Edasiste probleemide uurimiseks võib sul vaja minna ka järgmisi tööriistu.

- tcpdump,
- strace,
- lsof.

Neid kolme kirjeldatakse järgmisena selles õppetükis.

25.5. tcpdump

tcpdump prindib loogikaavaldisele vastava võrguliidese pakettide sisu kirjelduse.

Seda saab käitada ka **-w lipu** abil, mille tulemusel see salvestab paketi andmed hilisemaks analüüsimiseks faili ja/või **-r lippu**, mille tulemusel see loeb pigem salvestatud paketifailist kui pakette võrguliidesest.

Käsku „tcpdump“ kaitstakse Ubuntu jõustatava apparmor-profiili kaudu, mis piirab failide arvu, millele tcpdump võib juurde pääseda.

Igal juhul töötleb käsk „tcpdump“ ainult avaldisele vastavaid pakette. Salvestatud pakettide teavet saab edasi analüüsida Wiresharki abil.

Loe veel käsu „tcpdump“ kohta siit.

25.6. tcpdump (jätkub)

Allpool on antud mõned juhised tcpdumpi kasutamise kohta.

Paljusõnalise liiklusteabe vaatamiseks konkreetses võrguliideses konkreetsest hostist:

```
sudo tcpdump -i eth0 -n src
host <IP address> -v
```

Väga paljusõnalise liiklusteabe vaatamiseks konkreetses võrguliideses konkreetsest hostist portide 80 (HTTP) 443 (HTTPS) suunas:

```
sudo tcpdump -i eth0 -n “sr
c host <IP address> dst por
t 80 or dst port 443” -vvv
```

Iga vahetatud paketi vaatamiseks kasuta käsku -A. See käsk on käepärane veebilehtede hõivamiseks. Prindi iga pakett (v.a selle lingitasemel päis) ASCII-märgistikus.

Teabe kogumiseks, et Wireshark saaks seda analüüsida (käsk -s täismahus pakettide hõivamiseks):

```
sudo tcpdump -i eth0 -n src
host <IP address> -s 65535
 -w <some-file>
```

25.7. strace

„strace“ on diagnostika-, juhendav ja silumistööriist, mis aitab lahendada neid programmidega seotud probleeme, mille jaoks allikas pole kohe kätesaadav. Loe käsu „strace“ kohta siit.

Käsu käitamiseks strace'i abil localhosti kohta pingimiseks tee järgmist.

```
sudo strace ping localh
ost
```

Sel viisil on võimalik vaadata, milliseid teeke ja programme kasutatakse või mis on kaasatud konkreetse programmi käitamiseks. Pane tähele, et tavaline tagasiside, mida võid näha, on “No such file or directory” või “Resource temporarily unavailable”.

Ära muretse kuvatava teabe paljususe pärast. Leia aega esitatud andmete läbivaatamiseks ja tuvasta, kas vastav teave pole mingil põhjusel juurdepääsetav (nt puuduv või vigane konfiguratsioonifail).

PID-is töötava programmi jälitamiseks kasuta järgmist:

```
sudo strace -p 884
```

Protsessi PID-numbrid leiad, kui käitad:

```
sudo initctl list | gre
p "^xroad-"
```

Konkreetset võrguporti kuulava deemoni PID-numbri tuvastamiseks käita järgmine:

```
sudo netstat -anp|more
```

25.8. lsof

lsof loendab standardses väljundfailis teabe protsessi poolt avatud failide kohta. Avatud fail võib olla tavafail, kataloog, spetsiaalne plokkfail, spetsiaalne tärkfail, käivitatav tekstviide, teek, voo- või võrgufail (Interneti sokkel, NFS fail või UNIX domeenisokkel). Tee võib valida failisüsteemi ühe konkreetse faili või kõik failid.

Vormindatud kuva asemel annab Isof tulemuseks väljundi, mida saavad teised programmid sõeluda. Valikute puudumise korral loendab Isof kõik avatud failid, mis kuuluvad kõigisse aktiivsetesse protsessidesse.

Kõigi PID-i jaoks avatud ressurside loendamiseks tee järgmist.

```
sudo lsof -p 844
```

Kõigile kasutaja X-tee kasutamiseks avatud ressurside loendamiseks tee järgmist.

```
sudo lsof -u xroad
```

Loe Isofi kohta lähemalt siit.