IT BIZTONSÁG

6. forduló

A kategória támogatója: EURO ONE Számítástechnikai Zrt.

Ismertető a feladathoz

Log elemzés

Ajánlott programok: Linux paranccsor (grep, cut, sort, ...)

Felhasznált idő: 00:00/30:00 **Elért pontszám:** 0/15

Indítás utáni csatolmányok

1. feladat 0/5 pont

Az egyik webszolgáltató 1 nap hirtelen megnövekedett forgalmat tapasztaltak. Ez gyanús lett számukra, ezért megkértek, hogy az arra a napra vonatkozó szerver logokat elemezzük ki.

Melyik IP címtől érkezett a legtöbb kérés?

Válasz

A helyes válasz:

175.45.176.79

Magyarázat

$ cat nginx.log | cut -f1 -d " " | sort | uniq -c | sort -r | head -5

975 175.45.176.79 1 99.92.229.98 1 99.90.28.194 1 99.88.170.94 1 99.81.178.24

Innen látszik, hogy 975 kérés érkezett a 175.45.176.79 IP-től, ami a legtöbb.

2. feladat 0/2 pont

Melyik országból származik az IP cím?

Válaszok

A helyes válasz:

Észak-Korea

North Korea

Észak Korea

KP - Észak-Korea

Eszak-Korea

Korea (Democratic People's Republic of)

조선민주주의인민공화국 (Koreai Népi Demokratikus Köztársaság)

Phenjan, Phenjan, Észak-Korea

Pyongyang, Pyongyang, North Korea

Korea, Democratic People's Republic of

KP

Korea

Magyarázat

Az IP címhez az AS131279 Autonomous System szám tartozik.

3. feladat 0/4 pont

Mit csinált ez az IP cím?

Válasz

- ○ Túlterheléses támadást
- ○ XSS injekciót
- ◉ Brute force támadást
  Ez a válasz helyes, de nem jelölted meg.
- ○ Web scraping-et

Magyarázat

$ grep "175.45.176.79" nginx.log | grep "POST /login.php" | wc -l

572

Ebből a parancsból látszik, hogy 572 kérést indított az IP cím a bejelentkező oldal felé. Ha részletesebben megnézzük a logokat, látni lehet, hogy másod percenként érkezik egy kérés, valamint hogy a legtöbb kérés 403-as kóddal tér vissza, ami a “hozzáférés

megtagadva" HTTP kód. Ez azt jelenti, hogy a támadó valamilyen program használatával automatikusan végigment lehetséges bejelen tkezési adatokon, amit "brute force", azaz "nyers erő" támadásnak nevezünk.

4. feladat 0/4 pont

A logok alapján valószínűleg mit csinált még az IP cím?

Válasz

- (●) Letöltötte az összes email-t
  Ez a válasz helyes, de nem jelölted meg.
- ( ) Megváltoztatta az admin jelszót
- ( ) Fórumokra posztolt
- ( ) Semmit

Magyarázat

$ grep "175.45.176.79" nginx.log

... 175.45.176.79 - - [20/Apr/2022:13:14:19] "GET /email.php?id=1 HTTP/1.1" 200 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 "-" 0.967 0.778 . - 175.45.176.79 - - [20/Apr/2022:13:14:20] "GET /email.php?id=2 HTTP/1.1" 200 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 "-" 0.39 0.945 . - 175.45.176.79 - - [20/Apr/2022:13:14:21] "GET /email.php?id=3 HTTP/1.1" 200 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 "-" 0.297 0.273 . - 175.45.176.79 - - [20/Apr/2022:13:14:22] "GET /email.php?id=4 HTTP/1.1" 200 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 "-" 0.361 0.401 . - 175.45.176.79 - - [20/Apr/2022:13:14:23] "GET /email.php?id=5 HTTP/1.1" 200 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 "-" 0.596 0.815 . - 175.45.176.79 - - [20/Apr/2022:13:14:24] "GET /email.php?id=6 HTTP/1.1" 200 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 "-" 0.892 0.216 . - 175.45.176.79 - - [20/Apr/2022:13:14:25] "GET /email.php?id=7 HTTP/1.1" 200 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 "-" 0.606 0.669 . - 175.45.176.79 - - [20/Apr/2022:13:14:26] "GET /email.php?id=8 HTTP/1.1" 200 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 "-" 0.716 0.649 . - 2 175.45.176.79 - - [20/Apr/2022:13:14:27] "GET /email.php?id=9 HTTP/1.1" 200 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 "-" 0.912 0.099 . - 175.45.176.79 - - [20/Apr/2022:13:14:28] "GET /email.php?id=10 HTTP /1.1" 200 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko /20100101 Firefox/102.0 "-" 0.903 0.408 . - ...

Ezekből a log bejegyzésekből látható, hogy a támadó a /email.php végponton ment végig az "id" paraméteren egyesével. A kérések 1 másodpercre vannak egymástól, ebből valószínű, hogy a támadó egy automatizált program segít ségével végigment az email-eken.