**Ikke last ned 6.0 GB filen !!!!!!! den fucker opp hele splunk!**

Last ned MB versjonen av attack-only .tgz

Et bilde som inneholder tekst

Automatisk generert beskrivelse

**åpne**

**deretter splunk (program for å behandle data)**

**Husk gå på root for å starte/restarte splunk: sudo su –**

**Cd /opt og skriv = sudo /opt/splunk/bin/splunk start (eller restart)**

Et bilde som inneholder tekst

Automatisk generert beskrivelseindex=’’botsv1’’ earliest=0 all time

Del 2:

**Task 1**

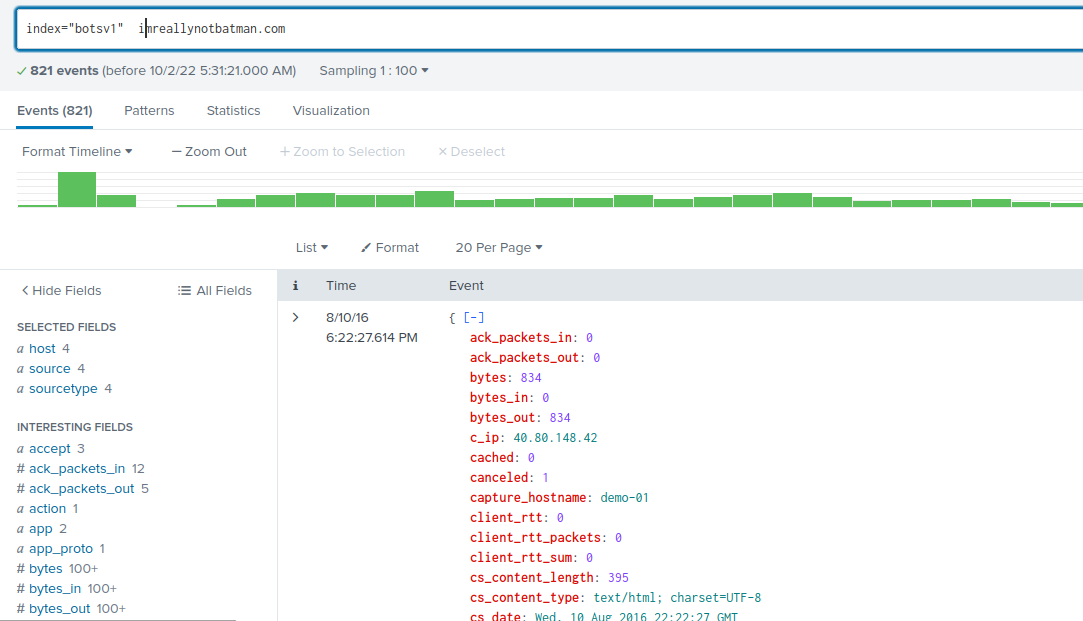
**What is the name of the company that makes the software that you are using for this competition? Just a six-letter word with no punctuation.**

**Ans: Splunk**

**Task 2**

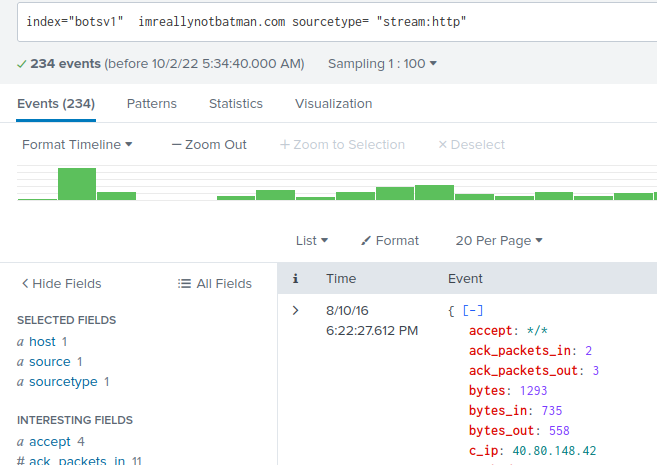
**What is the likely IP address of someone from the Po1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?**

Ans : skriver index = ‘’botsv1’’ imreallynotbatman.com



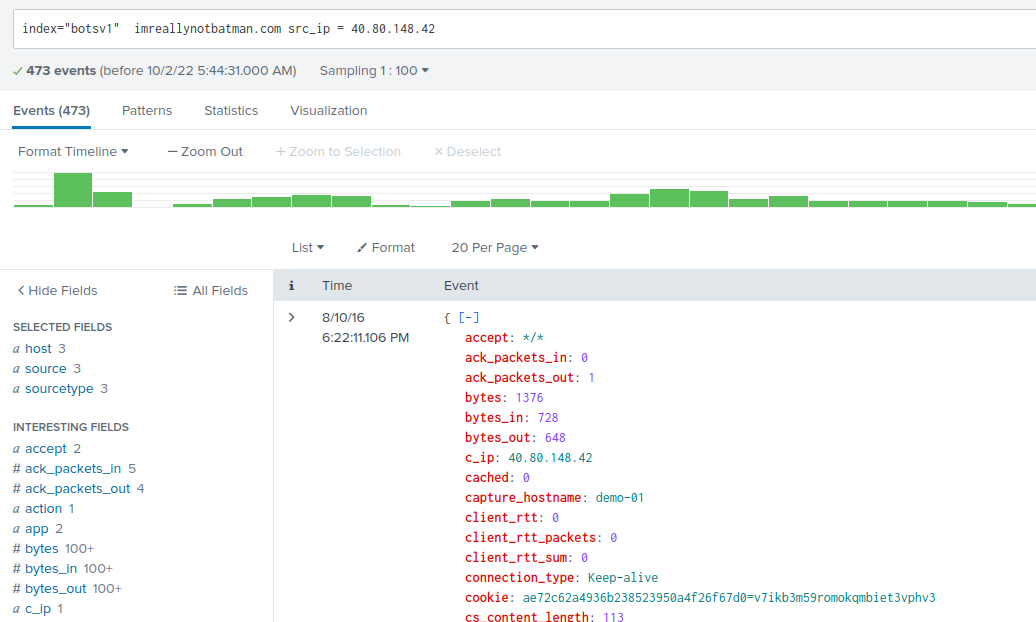
**Skriver index = ‘’botsv1’’ imreallynotbatman sourcetype ‘’source:http’’**

**Finner ip:**

****

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

****

**Task 3 :**

**What company created the web vulnerability scanner used by Po1s0n1vy? Type the company name. (For example, “Microsoft” or “Oracle”)**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**Ser de tre nest siste linjene :**

**Selskapet er Acunetix!**

**Task 4:**

**What content management system is imreallynotbatman.com likely using? (Please do not include punctuation such as. , ! ? in your answer. We are looking for alpha characters only.)**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

****

Imreallynotbatman.com is using joomla ( content management system for its website)

**Task 5:**

**What is the name of the file that defaced the imreallynotbatman.com website? Please submit only the name of the file with the extension (For example, “notepad.exe” or “favicon.ico”).**

**Trenger IP adressen til offeret:**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**Trykker på urlEt bilde som inneholder tekst

Automatisk generert beskrivelse**

**This attack used dynamic DNS to resolve the malicious IP. What is the fully qualified domain name (FQDN) associated with this attack?**

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Nettsiden heter : prankglassinbracket.jumpingcra.com