Elastic

Din descriere inteleg ca avem nevoie sa citim fisierele prezente in masina gazda asa ca daca intram pe url vedem ca agina web principală expune informații sensibile despre versiunea aplicației Elasticsearch.

Problema acum este ce facem avem un hint ca trebuie sa cautam ceva doar ca nu stiam la ce se referea am incercat sa folosesc dirsearch doar ca nu imi dadea ceva important so am cautat mai multe informatii despre Elasticsearch si mai ales despre versiunea acestuia.Am cautat cateva cve despre el si 3 au fost cele mai “bune” pentru noi.
1CVE-2015-1427: Această vulnerabilitate permite execuția de cod la distanță prin intermediul scripturilor Groovy nesecurizate. Atacatorii pot exploata această problemă pentru a executa comenzi arbitrare pe serverul care rulează Elasticsearch. Este recomandată actualizarea la o versiune ulterioară care remediază această problemă.

2.CVE-2015-5531: O vulnerabilitate de tip traversare de directoare în Elasticsearch înainte de versiunea 1.6.1 permite atacatorilor să citească fișiere arbitrare prin vectori nespecificați, legați de apelurile API de snapshot.

3.CVE-2015-5377: Această vulnerabilitate permite atacatorilor să execute cod arbitrar prin vectori nespecificați care implică protocolul de transport. Este recomandată actualizarea la versiunea 1.6.1 sau ulterioară pentru a remedia această problemă.

Doar ca cel mai convenabil din descriere si hint ar fi CVE-2015-5531 asa ca singurul lucru ramas pentru mine a fost sa caut un exploit specific.

https://github.com/nixawk/labs/blob/master/CVE-2015-5531/exploit.py (scriptul folosit).

[*] Usage: {} <elasticsearch_url> </etc/passwd>

Payloadul final:

python3 exploit.py http://35.246.139.54:32075/ /etc/passwd

Flag:

CTF{265b92ed0091f139fdcd438196…...14bce765bafd8344b1d96183e5}

Trolled by masquerade8077