Suceava CTF

Author: MTA 2

Bobeanu Catalina/Brinzea Andrei/Cujba Mihai/Lungu Andrei

Albania:

Summary

Proof of Flag

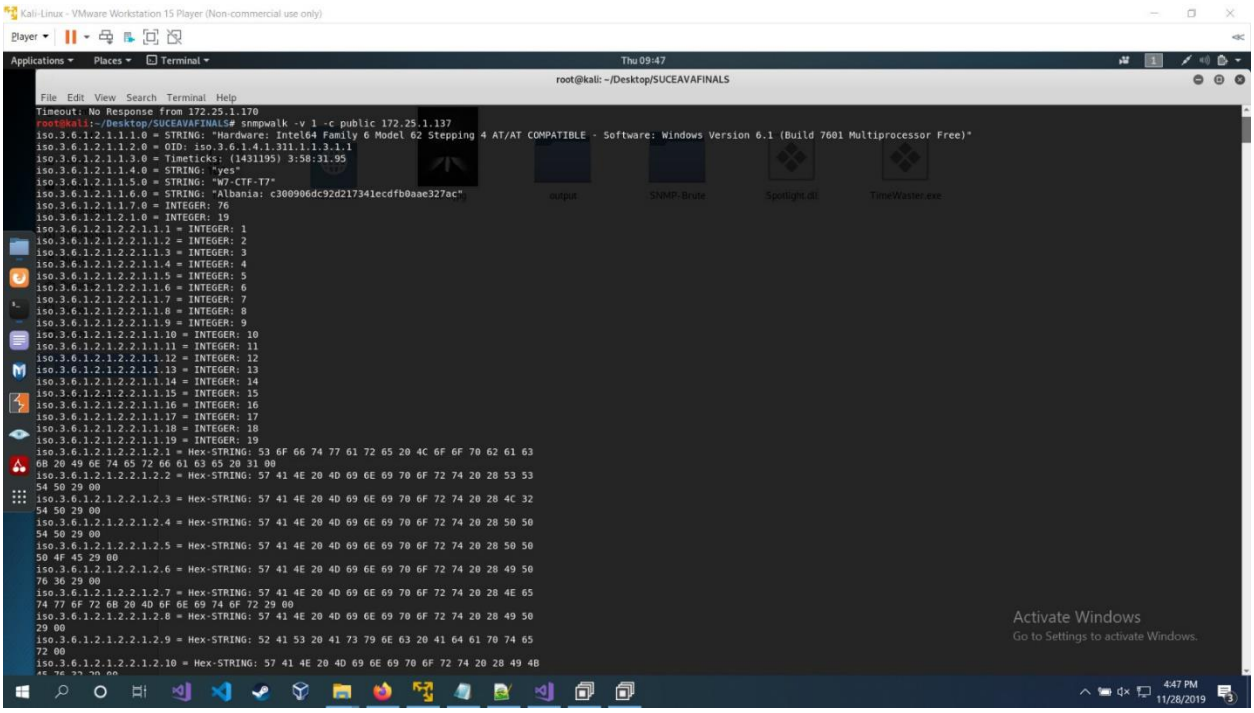
Albania: c300906dc92d217341ecdfb0aae327ac

Summary

Am gasit un port upd deschis, respective 161, pe care rula snmp.

Proof of Solving

snmpwalk -v 1 -c public 172.25.1.137



Croatia:

Summary

Proof of Flag

Croatia: dc7428b66c01ce3cb5362ea06ba05f09

Summary

Am gasit un port pe care rula CODIAD (portul 8024).

Proof of Solving

Cu gobuster am gasit un subdirector development in care se gasea un form de login pentru CODIAD. Aici am incercat user si parola default, admin admin si a mers. M-am uitat prin cele doua pagini si am vazut ca ultima functie de php se decripta dintr-un base64 din care iesea flag-ul

Australia:

Summary

Proof of Flag

Australia: c16b06e36c6401f77b2bb1bca3d0316b

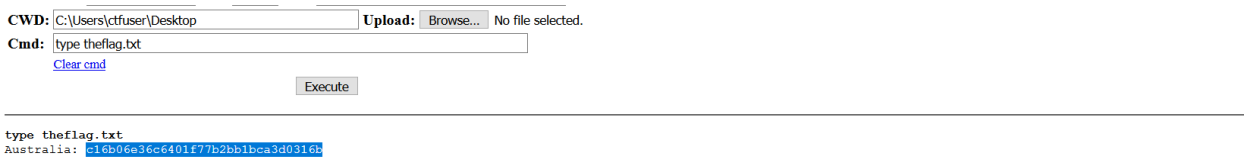
Summary

```
Am observant ca in CODIAD se pot rula scripturi php.
```

Proof of Solving

Odata ce puteam rula scripturi php ne-am uploadat 2 exploituri, p0wnyshell pentru a putea naviga mai usor prin directoare si inca unul pentru a putea uploada fisiere de pe masina locala (pentru prov. esc.)

Cu cel de-al doilea am putut sa ne conectam ca utilizator si sa citim flagul de pe Desktopul userului.



Italia:

Summary

Proof of Flag

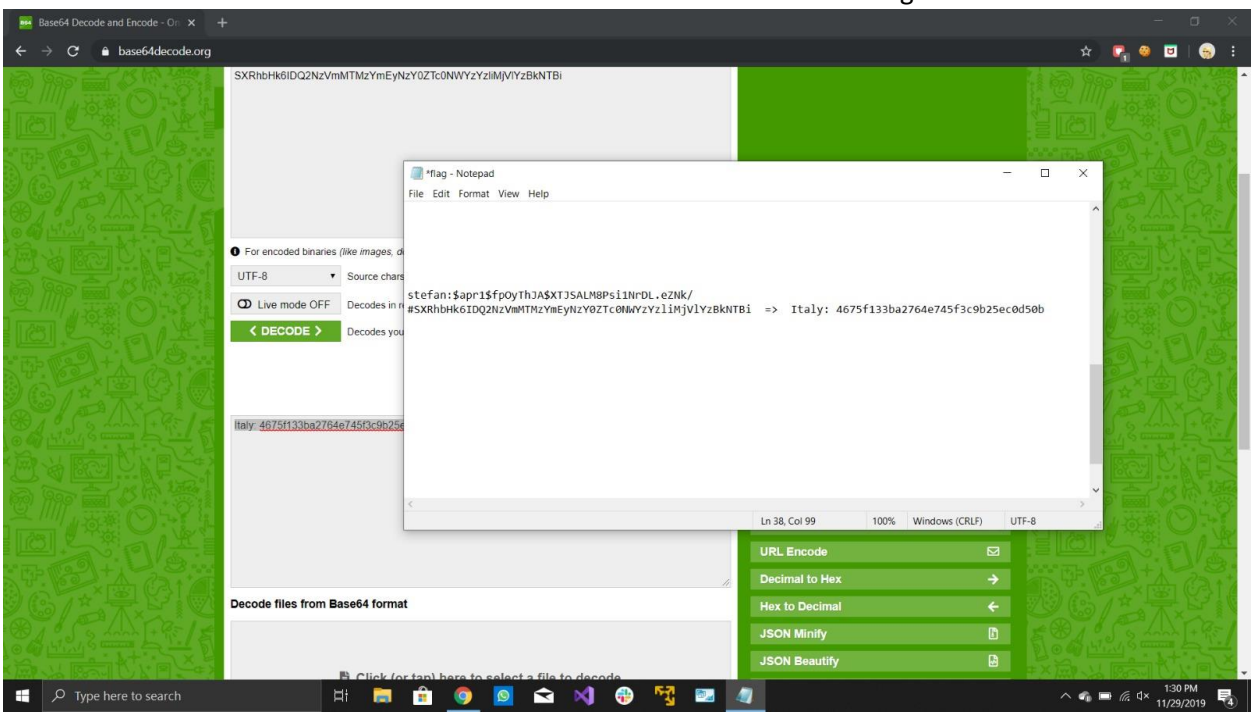
Italia: 4675f133ba2764e745f3c9b25ec0d50b

Summary

Avand drepturi de user am cautat prin xampp1 sa vedem ce utilizatori sunt inregistrati.

Proof of Solving

Am gasit un folder cu un utiluzator Stefan. Am incercat sa spargem hashul parolei, dar nu am reusit si am observat ca era delimitate de un alt base64. Acel base64 era flag-ul



China:

Summary

Proof of Flag

China: 30c509eeafe96e048742167938557f5a

Summary

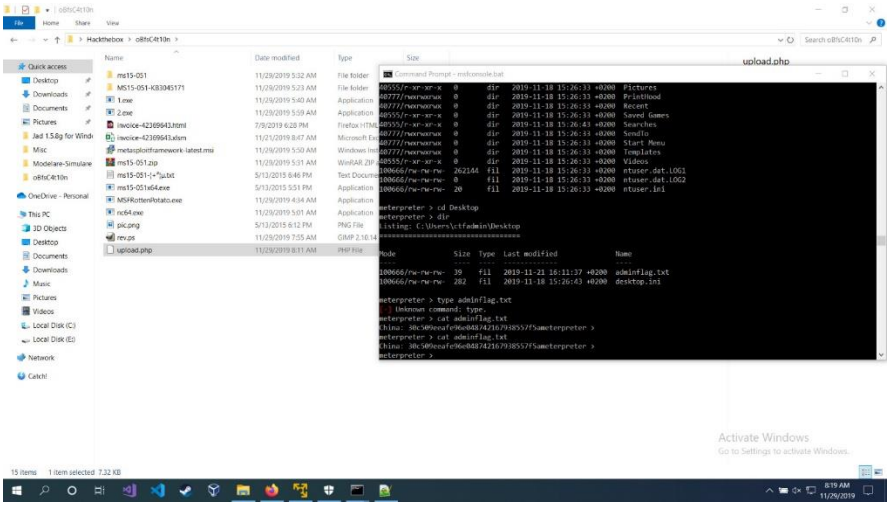
Am cautat un mod de a face priv. esc. Pentru a obtine coint de administrator.

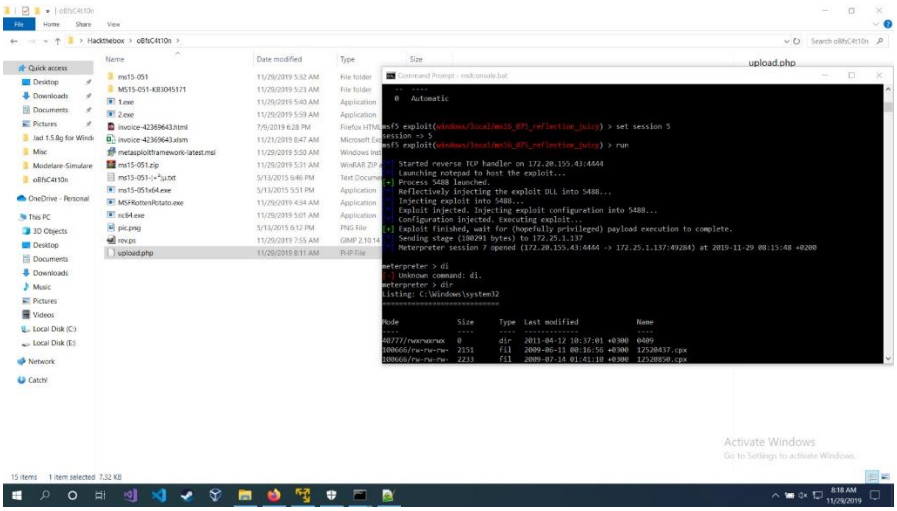
Proof of Solving

Am folosit utilitarul msf venom pentru a face un executabil ce creea un reverse shell pentru ip-ul me, pe portul 5555 odata ce era rulat.

De aici mi-am facut o sesiune de meterpreter, dar aveam privilegii de utilizator. Aici am pus meterpreterul in background si am folosit msfconsole pentru a cauta serverul de vulnerabilitati. Am gasit 4, dar doar una singura era valabila, respective ms16_075_reflection_juicy.

De aici ne-am folosit de sesiunea de meterpreter deja active pentru a exploata vulnerabilitatea. Dupa asta, am primit o sesiune noua ca administrator si am putut sa accesez flag-ul.




upload.php
Activate Windows
Go to Settings to activate Windows.