Pandora HTB

SNMP exploitation and sqlmap

Text

Description automatically generated

Found only 2 port open i.e ssh , http with ssh host-key. Thereby didn’t found much on website recon too.

Ran subdomain enumeration

Text

Description automatically generated with medium confidence

Found some js file in assets but nothing fancy yet,

Tried nmap scan again

Text

Description automatically generated

Interesting as snmp is known to send cleartext messages ,

To enumerate snmp information

Snmpwalk -v 1 -c public 10.10.11.136 > snmp1.txt

Text

Description automatically generated with medium confidence



Using the password ssh into pandora server

Setup proxychain

Graphical user interface, text

Description automatically generated

Text

Description automatically generated