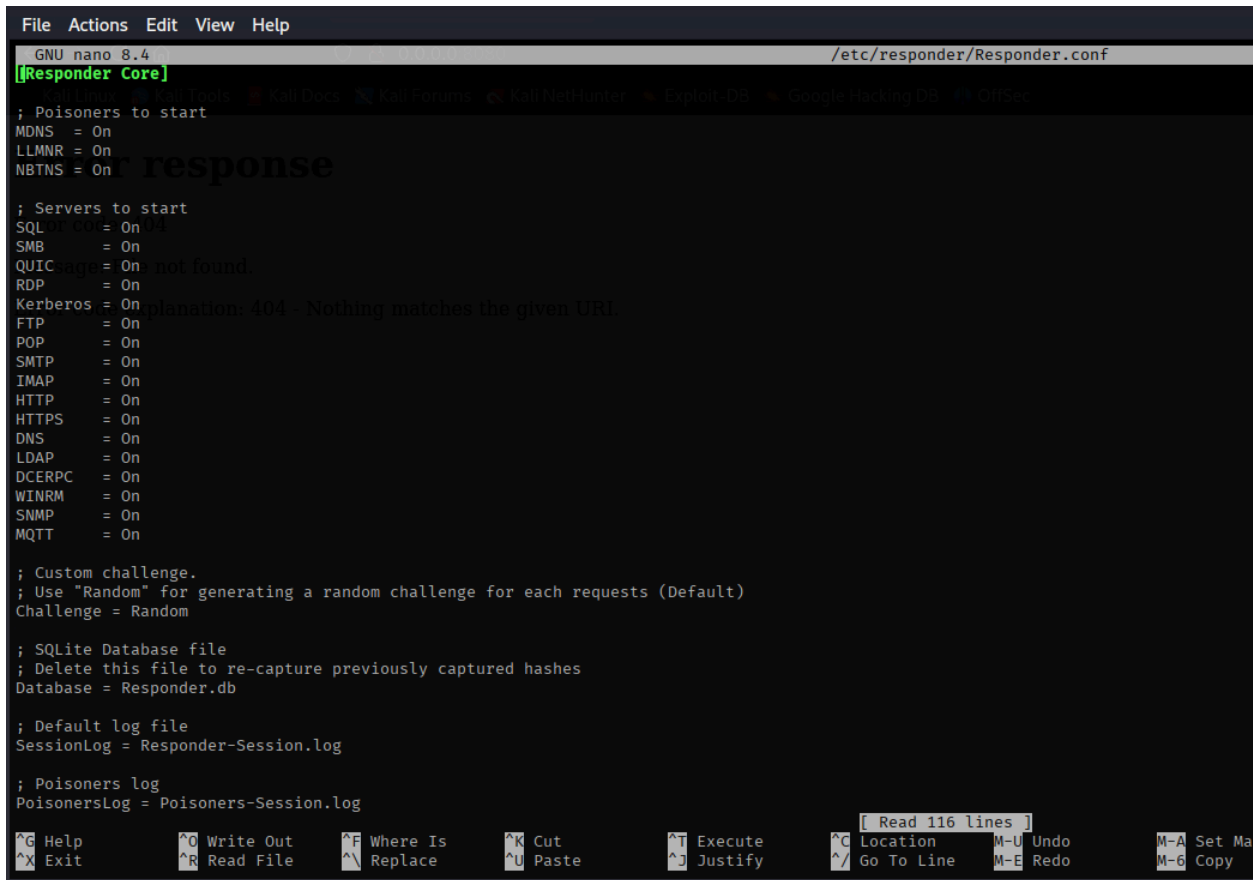


4. Network Protocol Attacks Lab

SMB Relay Attack Implementation

Tools: Responder, Ettercap, Wireshark, ntlmrelayx



The screenshot shows a terminal window with the nano text editor open, editing the file `/etc/responder/Responder.conf`. The editor's title bar indicates it is GNU nano 8.4. The configuration file content is as follows:

```
[Responder Core]
; Poisoners to start
MDNS = On
LLMNR = On
NBNS = On

; Servers to start
SQL = On
SMB = On
QUIC = On
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = On
HTTPS = On
DNS = On
LDAP = On
DCERPC = On
WINRM = On
SNMP = On
MQTT = On

; Custom challenge.
; Use "Random" for generating a random challenge for each requests (Default)
Challenge = Random

; SQLite Database file
; Delete this file to re-capture previously captured hashes
Database = Responder.db

; Default log file
SessionLog = Responder-Session.log

; Poisoners log
PoisonersLog = Poisoners-Session.log
```

The terminal also shows a web browser window in the background with the URL `http://192.168.1.200/` and a message: "planation: 404 - Nothing matches the given URL." The nano editor's status bar at the bottom shows various keyboard shortcuts like `^G Help`, `^X Exit`, `^O Write Out`, `^R Read File`, `^F Where Is`, `^N Replace`, `^K Cut`, `^U Paste`, `^T Execute`, `^J Justify`, `^C Location`, `^_ Go To Line`, `M-U Undo`, `M-E Redo`, `M-A Set Ma`, and `M-Q Copy`. A status indicator shows "[Read 116 lines]".

Attack ID	Technique	Target IP	Status	Outcome
015	SMB Relay	192.168.1.200	Success	NTLM Hash

Traffic Analysis

Implemented comprehensive Man-in-the-Middle attacks using Ettercap for ARP spoofing, captured authentication credentials, analyzed network patterns with Wireshark, demonstrating protocol vulnerabilities in enterprise environments.

Summary: Executed comprehensive MITM attacks intercepting network communications, capturing sensitive authentication data, and analyzing traffic patterns while demonstrating network protocol vulnerabilities.