

RELAY

- [Articles](#)
- [Relay Diagram](#)

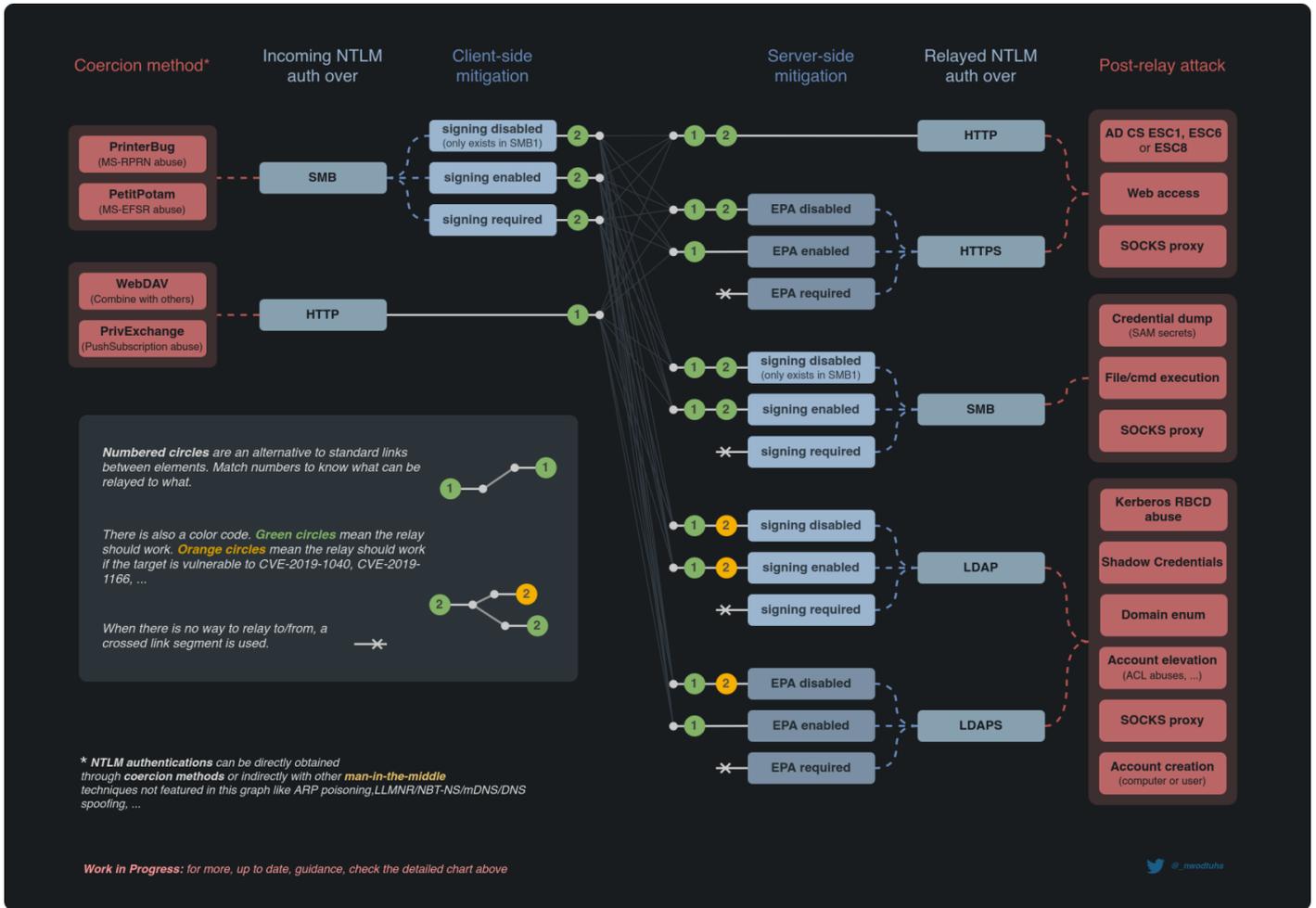
Articles

[TrustedSec | I'm bringing relaying back: A comprehensive guide on...](#)

[Relay | The Hacker Recipes](#)

Relay Diagram

Thanks [Relay | The Hacker Recipes](#)



		server												
		session signing						EPA						
		SMB1	HTTP	SMB1	SMB2	LDAP	SMB1/2 / LDAP	LDAPS	HTTPS	LDAPS	HTTPS	LDAPS / HTTPS		
		"disabled"	"not supported"	"enabled"	"not required"	"None"	"required"	"Never"	"Off"	"When supported"	"Accept"	"Always / Required"		
client	session signing	SMB1	"disabled"	✓	✓	✓	✓ 🍎	✓ 🚫	✗	✗ (ntlmrelay?)	✓	✓	?	✗
		HTTP	"not supported"	✓	✓	✓	✓ 🍎	✓	✗	✓	✓	✓	?	✗
		HTTP	"supported" (SMB1 and other Microsoft clients)	✓	✓	✓	✓ 🍎	✓	✗	✓	✗	✗	?	✗
		SMB1	"enabled"	✓	✓	✓	✓ 🍎	✓ 🚫	✗	✗ (ntlmrelay?)	✓	✗	?	✗
		SMB2	"not required"	✓	✓	✓	✓ 🍎	✓ 🚫	✗	✓ 🚫	✓	✗	?	✗
		SMB1	"required"	✓	✓	✓	✗ (ntlmrelay?)	✓ 🚫	✗	✗ (ntlmrelay?)	✓	✗	?	✗
		SMB2	"required"	✓ 🍎	✓ 🍎	✓ 🍎	✓ 🍎	✓ 🍎	✗	?	✓ 🍎	✗	?	✗

✗ it doesn't work
 ✓ it works
 🍎 enabling SMB2 support is needed (-smb2support)
 🚫 disabling multirelay (--no-multirelay) is needed (having only one target (-t) does that automatically)
 🚫 exploiting CVE-2019-1040 (--remove-mic) is needed (for unpatched targets only) or NTLMv1 (doesn't support MIC)
 * needs testing and/or confirmation
 ✗(ntlmrelay?) ntlmrelayx seemed faulty, needs to be tried again with network analysis