

AD

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

KRB

Articles

Protected Users Group

This is for when you are RESTRICTED or otherwise unable to do things due to being in the Protected Users group.

[Attacking Not-So-Protected User Sessions | Medium](#)

RELAY

RELAY

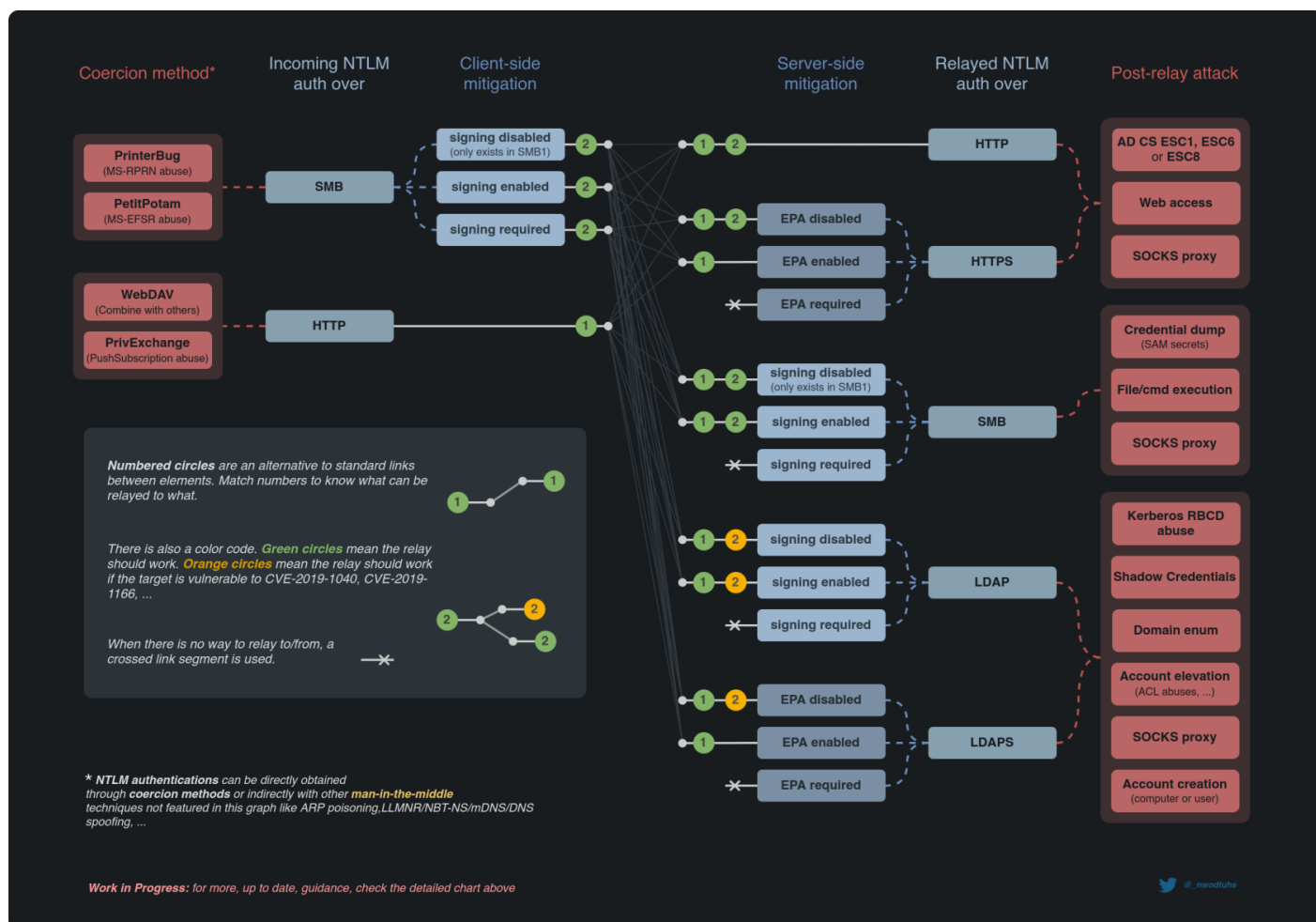
Articles

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

[Relay | The Hacker Recipes](#)

Relay Diagram

Thanks [Relay | The Hacker Recipes](#)



Work in Progress

			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"	✓	✓	✓	✓🍏	✓🔥	✗	✗ (ntlmrelayx?)	✓	✓	?	✗
		HTTP "not supported"	✓	✓	✓	✓🍏	✓	✗	✓	✓	✓	?	✗
		HTTP "supported" (WebDAV and other Microsoft clients)	✓	✓	✓	✓🍏	✓	✗	✓	✓	✗	?	✗
		SMB1 "enabled"	✓	✓	✓	✓🍏	✓🔥	✗	✗ (ntlmrelayx?)	✓	✗	?	✗
		SMB2 "not required"	✓	✓	✓	✓🍏	✓🔥	✗	✓🔥	✓	✗	?	✗
		SMB1 "required"	✓	✓	✓	✗ (ntlmrelayx?)	✓🔥	✗	✗ (ntlmrelayx?)	✓	✗	?	✗
		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

✗ (ntlmrelayx?) ntlmrelayx seemed faulty, needs to be tried again with network analysis

🐦 @_mawabute