AD

- KRB
  - Articles
- RELAY
  - Articles
  - Relay Diagram

KRB

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

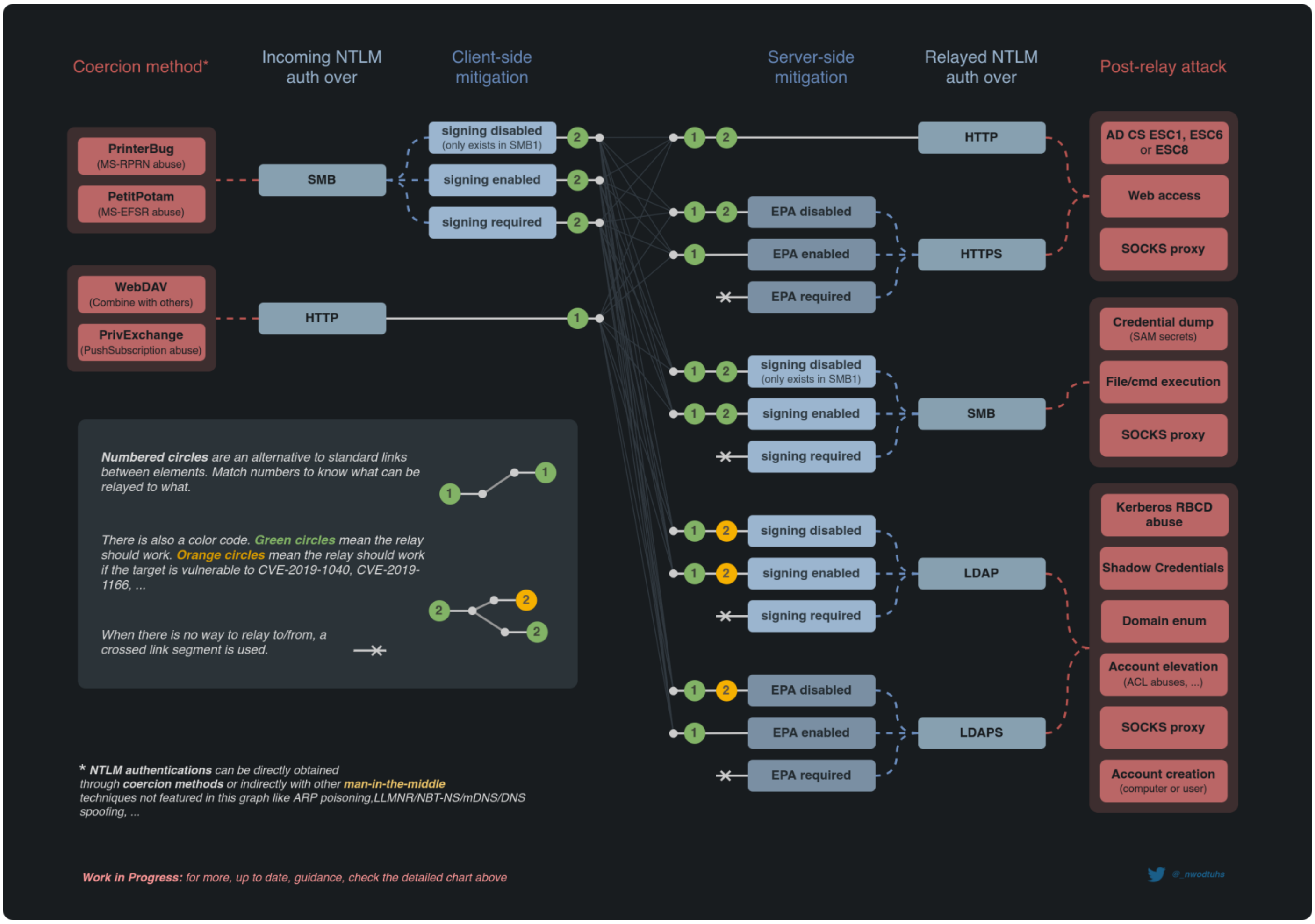
TrustedSec | I’m bringing relaying back: A comprehensive guide on…

Relay | The Hacker Recipes

RELAY

Relay Diagram

Thanks Relay | The Hacker Recipes



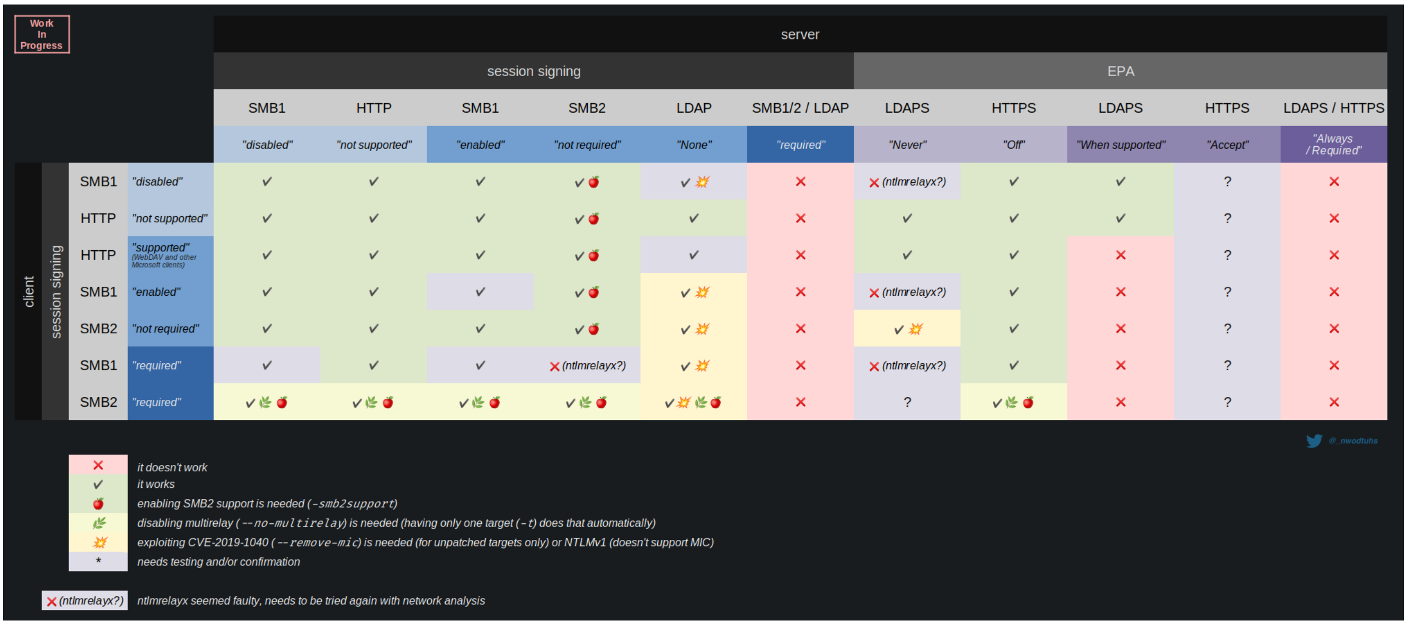
Numbered circles are an alternative to standard links between elements. Match numbers to know what can be relayed to what.

There is also a color code. *Green circles* mean the relay should work. *Orange circles* mean the relay should work if the target is vulnerable to CVE-2019-1040, CVE-2019-1166, ...

When there is no way to relay to/from, a crossed link segment is used.

* *NTLM authentications* can be directly obtained through *coercion methods* or indirectly with other *man-in-the-middle* techniques not featured in this graph like ARP poisoning,LLMNR/NBT-NS/mDNS/DNS spoofing, ...

Work in Progress: for more, up to date, guidance, check the detailed chart above



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"*	✓ 🌿 🍎	✓ 🌿 🍎	✓ 🌿 🍎	✓ 🌿 🍎	✓ 💥 🌿 🍎	✕	?	✓ 🌿 🍎	✕	?	✕

@_nwodtuhs

✕	*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*